TigerAccess™ EE

6-Band VDSL2 Switch

- 16 VDSL Downlink Ports (1 RJ-21 Connector)
- 2 Gigabit Ethernet Combination Ports (RJ-45/SFP)
- 1 Fast Ethernet Management Port (RJ-45)
- Non-blocking switching architecture
- Spanning Tree Protocol, RSTP, and MSTP
- Up to 12 LACP or static 8-port trunks
- Layer 2/3/4 CoS support through eight priority queues
- Layer 3/4 traffic priority with IP Precedence and IP DSCP
- Full support for VLANs with GVRP
- IGMP multicast filtering and snooping
- Manageable via console, Web, SNMP/RMON
- Security features: ACL, RADIUS, 802.1x
- VDSL line configuration using Long-Reach Ethernet (LRE) commands, line profiles, and alarm profiles

SMC® Networks

Management Guide

SMC7816M/VSW

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

TigerAccess™ EE Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC® Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

January 2007
Pub. # 149100012100H

Downloaded from www.Manualslib.com manuals search engine

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2007 by
SMC Networks, Inc.
20 Mason
Irvine, CA 92618
All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and EZ Switch, TigerAccess, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Downloaded from www.Manualslib.com manuals search engine

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at: **http://www.smc.com/index.cfm?action=customer_service_warranty**.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

Downloaded from www.Manualslib.com manuals search engine

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
20 Mason
Irvine, CA 92618

Downloaded from www.Manualslib.com manuals search engine

TABLE OF CONTENTS

Section I Getting Started

1 Introduction 1-1

Key Features 1-1
Description of Software Features 1-3
System Defaults 1-9

2 Initial Configuration 2-1

Connecting to the Switch 2-1
Configuration Options 2-1
Required Connections 2-2
Remote Connections 2-4
Basic Configuration 2-4
Console Connection 2-4
Setting Passwords 2-5
Setting an IP Address 2-6
Manual Configuration 2-8
Dynamic Configuration 2-9
Enabling SNMP Management Access 2-11
Community Strings (for SNMP version 1 and 2c clients) . 2-11
Trap Receivers 2-12
Configuring Access for SNMP Version 3 Clients 2-13
Managing System Files 2-14
Saving Configuration Settings 2-15

Section II Switch Management

3 Configuring the Switch 3-1

Using the Web Interface 3-1
Navigating the Web Browser Interface 3-3
Home Page 3-3
Configuration Options 3-4
Panel Display 3-4

Downloaded from www.Manualslib.com manuals search engine

Main Menu 3-5

4 Basic Management Tasks 4-1

Displaying System Information 4-1
Displaying System Health 4-4
Displaying Hardware/Software Versions 4-7
Displaying Bridge Extension Capabilities 4-9
Setting the Switch's IP Address 4-11
Manual Configuration 4-12
Using DHCP/BOOTP 4-14
Configuring Support for Jumbo Frames 4-16
Managing Firmware 4-17
Downloading System Software from a Server 4-18
Saving or Restoring Configuration Settings 4-20
Downloading Configuration Settings from a Server 4-22
Console Port Settings 4-24
Telnet Settings 4-26
Configuring Event Logging 4-29
System Log Configuration 4-29
Remote Log Configuration 4-31
Displaying Log Messages 4-33
Sending Simple Mail Transfer Protocol Alerts 4-34
Resetting the System 4-36
Setting the System Clock 4-37
Configuring SNTP 4-37
Setting the Time Zone 4-39

5 Simple Network Management Protocol 5-1

Enabling the SNMP Agent 5-4
Setting Community Access Strings 5-4
Specifying Trap Managers and Trap Types 5-6
Configuring SNMPv3 Management Access 5-10
Setting a Local Engine ID 5-10
Specifying a Remote Engine ID 5-11
Configuring SNMPv3 Users 5-12
Configuring Remote SNMPv3 Users 5-15
Configuring SNMPv3 Groups 5-18

Downloaded from www.Manualslib.com manuals search engine

Setting SNMPv3 Views 5-24

6 User Authentication 6-1

Configuring User Accounts 6-1
Configuring Local/Remote Logon Authentication 6-3
Configuring HTTPS 6-7
Replacing the Default Secure-site Certificate 6-9
Configuring the Secure Shell 6-10
Generating the Host Key Pair 6-13
Configuring the SSH Server 6-16
Configuring 802.1X Port Authentication 6-19
Displaying 802.1X Global Settings 6-21
Configuring 802.1X Global Settings 6-22
Configuring Port Settings for 802.1X 6-23
Displaying 802.1X Statistics 6-26
Filtering IP Addresses for Management Access 6-28

7 Client Security 7-1

Configuring Port Security 7-2
Configuring IP Source Guard 7-5
Configuring DHCP Snooping 7-8
Displaying DHCP Snooping Information 7-13
Configuring Packet Filtering 7-15
Filtering Service Packets 7-15
Filtering IP/MAC Address Pairs 7-18

8 Access Control Lists 8-1

Configuring Access Control Lists 8-1
Setting the ACL Name and Type 8-3
Configuring a Standard IP ACL 8-4
Configuring an Extended IP ACL 8-5
Configuring a MAC ACL 8-8
Configuring ACL Masks 8-10
Specifying the Mask Type 8-10
Configuring an IP ACL Mask 8-11
Configuring a MAC ACL Mask 8-14
Binding a Port to an Access Control List 8-16

Downloaded from www.Manualslib.com manuals search engine

9 Port Configuration 9-1
Displaying Connection Status 9-1
Configuring Interface Connections 9-4
Creating Trunk Groups 9-8
Statically Configuring a Trunk 9-9
Enabling LACP on Selected Ports 9-11
Configuring LACP Parameters 9-13
Displaying LACP Port Counters 9-17
Displaying LACP Settings and Status for the Local Side 9-18
Displaying LACP Settings and Status for the Remote Side . . . 9-21
Setting Broadcast Storm Thresholds 9-23
Configuring Port Mirroring 9-25
Configuring Rate Limits 9-26
Showing Port Statistics 9-29

10 VDSL Configuration 10-1
Configuring Global Settings for VDSL Ports 10-1
Configuring Interface Settings for VDSL Ports 10-7
Configuring Line Profiles 10-16
Displaying VDSL Status Information 10-21
Displaying VDSL Performance Statistics 10-25
Configuring an Alarm Profile 10-30
Displaying CPE Information 10-36
Configuring OAM Functions and Upgrading CPE Firmware 10-41

11 Address Table Settings 11-1
Setting Static Addresses 11-1
Displaying the Address Table 11-2
Changing the Aging Time 11-4

12 Spanning Tree Algorithm 12-1
Displaying Global Settings 12-4
Configuring Global Settings 12-8
Displaying Interface Settings 12-13
Configuring Interface Settings 12-18
Configuring Multiple Spanning Trees 12-22
Displaying Interface Settings for MSTP 12-25

Downloaded from www.Manualslib.com manuals search engine

Configuring Interface Settings for MSTP 12-27

13 VLAN Configuration 13-1

Selecting the VLAN Operation Mode 13-1
IEEE 802.1Q VLANs 13-2
Enabling or Disabling GVRP (Global Setting) 13-6
Displaying Basic VLAN Information 13-7
Displaying Current VLANs 13-8
Creating VLANs 13-10
Adding Static Members to VLANs (VLAN Index) 13-12
Adding Static Members to VLANs (Port Index) 13-14
Configuring VLAN Behavior for Interfaces 13-15
Configuring Private VLANs 13-18
Enabling Private VLANs 13-18
Configuring Uplink and Downlink Ports 13-19
Configuring Protocol-Based VLANs 13-20
Configuring Protocol Groups 13-21
Mapping Protocols to VLANs 13-22
Configuring IEEE 802.1Q Tunneling 13-24
Adding an Interface to a QinQ Tunnel 13-30
Configuring VLAN Swapping 13-33

14 Class of Service 14-1

Layer 2 Queue Settings 14-1
Setting the Default Priority for Interfaces 14-1
Mapping CoS Values to Egress Queues 14-3
Selecting the Queue Mode 14-6
Setting the Service Weight for Traffic Classes 14-7
Layer 3/4 Priority Settings 14-9
Mapping Layer 3/4 Priorities to CoS Values 14-9
Selecting IP Precedence/DSCP Priority 14-10
Mapping IP Precedence 14-11
Mapping DSCP Priority 14-13
Mapping IPv6 Traffic Classes 14-15
Mapping IP Port Priority 14-16

Downloaded from www.Manualslib.com manuals search engine

15 Quality of Service 15-1
Configuring Quality of Service Parameters 15-2
Configuring a Class Map 15-3
Creating QoS Policies 15-6
Attaching a Policy Map to Ingress Queues 15-10

16 Multicast Filtering 16-1
Layer 2 IGMP (Snooping and Query) 16-2
Configuring IGMP Snooping and Query Parameters 16-4
Displaying Interfaces Attached to a Multicast Router 16-7
Specifying Static Interfaces for a Multicast Router 16-8
Displaying Port Members of Multicast Services 16-9
Assigning Ports to Multicast Services 16-11
Configuring Immediate Leave from Multicast Groups 16-13
IGMP Filtering and Throttling 16-14
Enabling IGMP Filtering and Throttling 16-15
Configuring IGMP Filter Profiles 16-16
Configuring IGMP Filtering and Throttling for Interfaces . . 16-18
Multicast VLAN Registration 16-20
Configuring Global MVR Settings 16-21
Displaying MVR Interface Status 16-24
Configuring MVR Interfaces 16-26
Displaying Port Members of Multicast Groups 16-28
Assigning Static Multicast Groups to Interfaces 16-30

17 Domain Name Service 17-1
Configuring General DNS Service Parameters 17-1
Configuring Static DNS Host to Address Entries 17-4
Displaying the DNS Cache 17-6

Section III Command Line Interface

18 Overview of the Command Line Interface 18-1
Using the Command Line Interface 18-1
Accessing the CLI 18-1

Downloaded from www.Manualslib.com manuals search engine

Console Connection 18-1
Telnet Connection 18-2
Entering Commands 18-3
Keywords and Arguments 18-3
Minimum Abbreviation 18-4
Command Completion 18-4
Getting Help on Commands 18-4
Showing Commands 18-5
Partial Keyword Lookup 18-6
Negating the Effect of Commands 18-6
Using Command History 18-7
Understanding Command Modes 18-7
Exec Commands 18-8
Configuration Commands 18-8
Command Line Processing 18-11
Command Groups 18-12

19 General Commands 19-1

enable 19-2
disable 19-3
configure 19-3
show history 19-4
reload 19-5
prompt 19-6
end 19-6
exit 19-7
quit 19-7

20 System Management Commands 20-1

Device Designation Commands 20-2
hostname 20-2
System Status Commands 20-3
show startup-config 20-3
show running-config 20-6
show system 20-8
show users 20-9
show version 20-10

Downloaded from www.Manualslib.com manuals search engine

show bme version 20-10
show cpu utilization 20-11
show memory status 20-12
System Mode Commands 20-13
system mode 20-13
show system mode 20-14
Frame Size Commands 20-15
jumbo frame 20-15
File Management Commands 20-16
copy 20-17
delete 20-22
dir 20-23
whichboot 20-24
boot system 20-25
Line Commands 20-26
line 20-27
login 20-28
password 20-29
timeout login response 20-30
exec-timeout 20-31
password-thresh 20-32
silent-time 20-33
databits 20-33
parity 20-34
speed 20-35
stopbits 20-36
disconnect 20-36
show line 20-37
Event Logging Commands 20-39
logging on 20-39
logging history 20-40
logging host 20-41
logging facility 20-42
logging trap 20-43
clear log 20-44
show logging 20-45
show log 20-47

Downloaded from www.Manualslib.com manuals search engine

SMTP Alert Commands 20-48
logging sendmail host 20-48
logging sendmail level 20-49
logging sendmail source-email 20-50
logging sendmail destination-email 20-50
logging sendmail 20-51
show logging sendmail 20-52
Time Commands 20-53
sntp client 20-53
sntp server 20-54
sntp poll 20-55
show sntp 20-56
clock timezone 20-57
calendar set 20-58
show calendar 20-58

21 SNMP Commands 21-1

snmp-server 21-2
show snmp 21-3
snmp-server community 21-4
snmp-server contact 21-5
snmp-server location 21-5
snmp-server host 21-6
snmp-server enable traps 21-9
snmp-server engine-id 21-10
show snmp engine-id 21-12
snmp-server view 21-13
show snmp view 21-14
snmp-server group 21-15
show snmp group 21-16
snmp-server user 21-18
show snmp user 21-20

22 User Authentication Commands 22-1

User Account Commands 22-2
username 22-2
enable password 22-4

Downloaded from www.Manualslib.com manuals search engine

Authentication Sequence 22-5
authentication login 22-5
authentication enable 22-7
RADIUS Client 22-8
radius-server host 22-9
radius-server port 22-10
radius-server key 22-10
radius-server retransmit 22-11
radius-server timeout 22-11
show radius-server 22-12
TACACS+ Client 22-13
tacacs-server host 22-13
tacacs-server port 22-14
tacacs-server key 22-14
show tacacs-server 22-15
Web Server Commands 22-15
ip http port 22-16
ip http server 22-16
ip http secure-server 22-17
ip http secure-port 22-18
Telnet Server Commands 22-20
ip telnet server 22-20
Secure Shell Commands 22-21
ip ssh server 22-25
ip ssh timeout 22-26
ip ssh authentication-retries 22-27
ip ssh server-key size 22-27
delete public-key 22-28
ip ssh crypto host-key generate 22-28
ip ssh crypto zeroize 22-29
ip ssh save host-key 22-30
show ip ssh 22-31
show ssh 22-31
show public-key 22-32
802.1X Port Authentication 22-34
dot1x system-auth-control 22-35
dot1x default 22-35

Downloaded from www.Manualslib.com manuals search engine

dot1x max-req 22-36
dot1x port-control 22-36
dot1x operation-mode 22-37
dot1x re-authenticate 22-38
dot1x re-authentication 22-39
dot1x timeout quiet-period 22-39
dot1x timeout re-authperiod 22-40
dot1x timeout tx-period 22-41
show dot1x 22-41
Management IP Filter Commands 22-45
management 22-45
show management 22-46

23 Client Security Commands 23-1

Port Security Commands 23-2
port security 23-3
Packet Filtering Commands 23-5
filter ipmac 23-5
filter netbios 23-7
filter dhcp-request 23-8
filter dhcp 23-9
show filter 23-10
IP Source Guard Commands 23-11
ip source-guard 23-11
ip source-guard binding 23-14
show ip source-guard 23-15
show ip source-guard binding 23-16
DHCP Snooping Commands 23-17
ip dhcp snooping 23-18
ip dhcp snooping vlan 23-20
ip dhcp snooping verify mac-address 23-21
ip dhcp snooping database write 23-22
ip dhcp snooping service-provider-mode 23-22
ip dhcp snooping client limit 23-23
ip dhcp snooping trust 23-24
show ip dhcp snooping 23-25
show ip dhcp snooping binding 23-26

Downloaded from www.Manualslib.com manuals search engine

24 Access Control List Commands 24-1

IP ACLs 24-2
- access-list ip 24-3
- permit, deny (Standard IP ACL) 24-4
- permit, deny (Extended IP ACL) 24-5
- show ip access-list 24-7
- access-list ip mask-precedence 24-8
- mask (IP ACL) 24-9
- show access-list ip mask-precedence 24-14
- ip access-group 24-14
- show ip access-group 24-15

MAC ACLs 24-16
- access-list mac 24-17
- permit, deny (MAC ACL) 24-18
- show mac access-list 24-20
- access-list mac mask-precedence 24-20
- mask (MAC ACL) 24-21
- show access-list mac mask-precedence 24-24
- mac access-group 24-25
- show mac access-group 24-26

ACL Information 24-26
- show access-list 24-26
- show access-group 24-27

25 Interface Commands 25-1

interface 25-2
description 25-3
speed-duplex 25-3
negotiation 25-5
capabilities 25-6
flowcontrol 25-7
media-type 25-8
switchport mdix 25-9
shutdown 25-10
switchport packet-rate 25-11
clear counters 25-12
show interfaces status 25-13

Downloaded from www.Manualslib.com manuals search engine

show interfaces counters 25-14
show interfaces switchport 25-16

26 Link Aggregation Commands 26-1

channel-group 26-3
lacp 26-4
lacp system-priority 26-6
lacp admin-key (Ethernet Interface) 26-7
lacp admin-key (Port Channel) 26-8
lacp port-priority 26-9
show lacp 26-10

27 Mirror Port Commands 27-1

port monitor 27-1
show port monitor 27-2

28 Rate Limit Commands 28-1

rate-limit 28-2
rate-limit trap-input 28-3
show rate-limit vlan 28-4

29 VDSL Commands 29-1

Long-Reach Ethernet Commands 29-2
lre band-plan 29-4
lre option-band 29-6
lre ham-band 29-7
lre region-ham-band 29-9
lre psd-breakpoints 29-12
lre psd-frequencies 29-13
lre psd-value 29-15
lre psd-mask-level 29-16
lre pbo-config 29-18
lre upbo 29-19
lre tone 29-21
lre max-power 29-22
lre min-protection 29-23
lre channel 29-24

Downloaded from www.Manualslib.com manuals search engine

lre interleave-max-delay 29-25
lre datarate 29-26
lre rate-set 29-27
lre noise-mgn target 29-28
lre noise-mgn min 29-29
lre shutdown 29-30
lre reset 29-30
lre auto-retraining 29-31
lre retraining 29-32
lre rate-adaption 29-33
lre apply 29-34
Line Profile Commands 29-35
line-profile 29-36
lre line-profile 29-37
band-plan 29-38
option-band 29-39
ham-band 29-40
region-ham-band 29-41
tone 29-42
max-power 29-43
min-protection 29-44
channel 29-45
down/up-max-inter-delay 29-46
down/up-fast/slow-max/min-datarate 29-47
down/up-target-noise-mgn 29-48
down/up-min-noise-mgn 29-49
Alarm Profile Commands 29-51
alarm-profile 29-52
lre alarm-profile 29-52
init-failure 29-53
thresh-15min-ess 29-54
thresh-15min-lofs 29-55
thresh-15min-lols 29-56
thresh-15min-loss 29-57
thresh-15min-lprs 29-58
thresh-15min-sess 29-59
thresh-15min-uass 29-60

Downloaded from www.Manualslib.com manuals search engine

Displaying VDSL Information 29-61
show lre band-plan 29-62
show lre option-band 29-63
show lre ham-band 29-64
show lre region-ham-band 29-65
show lre psd 29-67
show lre psd-mask-level 29-68
show lre pbo-config 29-69
show lre upbo 29-70
show lre tone 29-71
show lre interleave-max-delay 29-72
show lre datarate 29-73
show lre noise-mgn 29-74
show lre rate-adaption 29-75
show lre config 29-76
show lre line-profile 29-77
show lre alarm-profile 29-78
show lre 29-79
show lre phys-info 29-80
show lre rate-info 29-81
show lre perf 29-82
CPE Configuration 29-86
oam local clear counter 29-86
efm remote eeprom-write 29-87
copy tftp firmware 29-87
oam remote upgrade firmware 29-90
oam remote firmware active 29-90
show cpe-info 29-91

30 Address Table Commands 30-1

mac-address-table static 30-2
clear mac-address-table dynamic 30-3
show mac-address-table 30-4
mac-address-table aging-time 30-5
show mac-address-table aging-time 30-6

Downloaded from www.Manualslib.com manuals search engine

31 Spanning Tree Commands 31-1

spanning-tree 31-3
spanning-tree mode 31-4
spanning-tree forward-time 31-5
spanning-tree hello-time 31-6
spanning-tree max-age 31-7
spanning-tree priority 31-8
spanning-tree pathcost method 31-9
spanning-tree transmission-limit 31-10
spanning-tree mst-configuration 31-10
mst vlan 31-11
mst priority 31-12
name 31-13
revision 31-14
max-hops 31-14
spanning-tree spanning-disabled 31-15
spanning-tree cost 31-16
spanning-tree port-priority 31-18
spanning-tree edge-port 31-18
spanning-tree portfast 31-19
spanning-tree link-type 31-21
spanning-tree mst cost 31-22
spanning-tree mst port-priority 31-23
spanning-tree protocol-migration 31-24
show spanning-tree 31-25
show spanning-tree mst configuration 31-27

32 VLAN Commands 32-1

GVRP and Bridge Extension Commands 32-2
bridge-ext gvrp 32-2
show bridge-ext 32-3
switchport gvrp 32-4
show gvrp configuration 32-4
garp timer 32-5
show garp timer 32-6
Editing VLAN Groups 32-7
vlan database 32-7

Downloaded from www.Manualslib.com manuals search engine

vlan 32-8
Configuring VLAN Interfaces 32-9
interface vlan 32-9
switchport mode 32-10
switchport acceptable-frame-types 32-11
switchport ingress-filtering 32-12
switchport native vlan 32-13
switchport allowed vlan 32-14
switchport forbidden vlan 32-15
Displaying VLAN Information 32-16
show vlan 32-16
Configuring Private VLANs 32-17
pvlan 32-17
show pvlan 32-19
Configuring Protocol-based VLANs 32-20
protocol-vlan protocol-group (Configuring Groups) 32-21
protocol-vlan protocol-group (Configuring Interfaces) 32-22
show protocol-vlan protocol-group 32-23
show interfaces protocol-vlan protocol-group 32-24
Configuring IEEE 802.1Q Tunneling 32-25
qinq priority map 32-26
switchport mode dot1q-tunnel 32-27
show dot1q-tunnel 32-28
switchport dot1q-ethertype 32-29
Configuring VLAN Swapping 32-30
switchport vlan swap 32-31
show vlan-swap 32-32

33 Class of Service Commands 33-1

Priority Commands (Layer 2) 33-1
priority bits 33-2
queue mode 33-3
show priority 33-4
show queue mode 33-5
switchport priority default 33-5
queue bandwidth 33-7
queue cos-map 33-8

Downloaded from www.Manualslib.com manuals search engine

show queue bandwidth 33-9
show queue cos-map 33-10
Priority Commands (Layer 3 and 4) 33-11
map ip port (Global Configuration) 33-12
map ip port (Interface Configuration) 33-12
map ip precedence (Global Configuration) 33-13
map ip precedence (Interface Configuration) 33-14
map ip dscp (Global Configuration) 33-15
map ip dscp (Interface Configuration) 33-16
priority ipv6 33-17
show map ip port 33-18
show map ip precedence 33-19
show map ip dscp 33-20

34 Quality of Service Commands 34-1

class-map 34-3
match 34-4
policy-map 34-6
class 34-7
set 34-8
police 34-9
service-policy 34-10
show class-map 34-11
show policy-map 34-12
show policy-map interface 34-12

35 Multicast Filtering Commands 35-1

IGMP Snooping Commands 35-2
ip igmp snooping 35-2
ip igmp snooping vlan static 35-3
ip igmp snooping version 35-4
ip igmp snooping immediate-leave 35-5
show ip igmp snooping 35-6
show mac-address-table multicast 35-6
IGMP Query Commands 35-7
ip igmp snooping querier 35-8
ip igmp snooping query-count 35-8

Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping query-interval 35-9
ip igmp snooping query-max-response-time 35-10
ip igmp snooping router-port-expire-time 35-11
Static Multicast Routing Commands 35-12
ip igmp snooping vlan mrouter 35-12
show ip igmp snooping mrouter 35-13
IGMP Filtering and Throttling Commands 35-14
ip igmp filter (Global Configuration) 35-15
ip igmp profile 35-16
permit, deny 35-16
range 35-17
ip igmp filter (Interface Configuration) 35-18
ip igmp max-groups 35-18
ip igmp max-groups action 35-19
show ip igmp filter 35-20
show ip igmp profile 35-21
show ip igmp throttle interface 35-22
Multicast VLAN Registration Commands 35-23
mvr (Global Configuration) 35-24
mvr (Interface Configuration) 35-26
mvr immediate 35-28
show mvr 35-29

36 Domain Name Service Commands 36-1

ip host 36-2
clear host 36-3
ip domain-name 36-4
ip domain-list 36-5
ip name-server 36-6
ip domain-lookup 36-7
show hosts 36-8
show dns 36-9
show dns cache 36-9
clear dns cache 36-10

Downloaded from www.Manualslib.com manuals search engine

37 DHCP Commands 37-1

DHCP Client 37-1
ip dhcp restart client 37-1
DHCP Relay 37-2
ip dhcp relay server 37-3
ip dhcp information option 37-4
ip dhcp information policy 37-6
show ip dhcp relay server 37-7
. 37-8

38 IP Interface Commands 38-1

Basic IP Configuration 38-1
ip address 38-2
ip default-gateway 38-3
show ip interface 38-4
show ip redirects 38-4
ping 38-5

Downloaded from www.Manualslib.com manuals search engine

Section IV Appendices

A Software Specifications A-1

Software Features A-1
Management Features A-3
Standards A-3
Management Information Bases A-4

B Troubleshooting B-1

Problems Accessing the Management Interface B-1
Using System Logs B-3

Glossary

Index

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

TABLES

Table 1-1 Key Features 1-1
Table 1-2 System Defaults 1-9
Table 3-1 Web Page Configuration Buttons 3-4
Table 3-2 Switch Main Menu 3-5
Table 4-1 Logging Levels 4-29
Table 5-1 SNMPv3 Security Models and Levels 5-2
Table 5-2 Supported Notification Messages 5-19
Table 6-1 HTTPS System Support 6-8
Table 6-2 802.1X Statistics 6-26
Table 9-1 LACP Port Counters 9-17
Table 9-2 LACP Internal Configuration Information 9-18
Table 9-3 LACP Neighbor Configuration Information 9-21
Table 9-4 Port Statistics 9-29
Table 10-1 LRE Status 10-21
Table 10-2 Rate Status 10-22
Table 10-3 Error Statistics 10-25
Table 10-4 Ethernet Receive Performance Counters 10-25
Table 10-5 Ethernet Transmit Performance Counters 10-26
Table 10-6 H.D.L.C. Performance Counters 10-27
Table 10-7 CPE Firmware Versions 10-36
Table 10-8 CO Firmware Buffer Information 10-36
Table 10-9 CPE Performance Counters 10-37
Table 12-1 Recommended STA Path Cost Range 12-19
Table 12-2 Recommended STA Path Costs 12-19
Table 14-1 Mapping CoS Values to Egress Queues 14-3
Table 14-2 CoS Priority Levels 14-4
Table 14-3 Mapping IP Precedence 14-11
Table 14-4 Mapping DSCP Priority 14-13
Table 18-1 General Command Modes 18-7
Table 18-2 Configuration Command Modes 18-10
Table 18-3 Keystroke Commands 18-11
Table 18-4 Command Group Index 18-12
Table 19-1 General Commands 19-1
Table 20-1 System Management Commands 20-1
Table 20-2 Device Designation Commands 20-2
Table 20-3 System Status Commands 20-3

Downloaded from www.Manualslib.com manuals search engine

Table 20-4 show bme version - display description 20-11
Table 20-5 show cpu utilization - display description 20-12
Table 20-7 System Mode Commands 20-13
Table 20-6 show memory status - display description 20-13
Table 20-8 Frame Size Commands 20-15
Table 20-9 Flash/File Commands 20-16
Table 20-10 File Directory Information 20-23
Table 20-11 Line Commands 20-26
Table 20-12 Event Logging Commands 20-39
Table 20-13 Logging Levels 20-40
Table 20-14 show logging flash/ram - display description 20-46
Table 20-15 show logging trap - display description 20-46
Table 20-16 SMTP Alert Commands 20-48
Table 20-17 Time Commands 20-53
Table 21-1 SNMP Commands 21-1
Table 21-2 show snmp engine-id - display description 21-12
Table 21-3 show snmp view - display description 21-14
Table 21-4 show snmp group - display description 21-17
Table 21-5 show snmp user - display description 21-20
Table 22-1 Authentication Commands 22-1
Table 22-2 User Access Commands 22-2
Table 22-3 Default Login Settings 22-3
Table 22-4 Authentication Sequence Commands 22-5
Table 22-5 RADIUS Client Commands 22-8
Table 22-6 TACACS+ Client Commands 22-13
Table 22-7 Web Server Commands 22-15
Table 22-8 HTTPS System Support 22-18
Table 22-9 Telnet Server Commands 22-20
Table 22-10 Secure Shell Commands 22-21
Table 22-11 show ssh - display description 22-31
Table 22-12 802.1X Port Authentication Commands 22-34
Table 22-13 Management IP Filter Commands 22-45
Table 23-1 Client Security Commands 23-2
Table 23-2 Port Security Commands 23-3
Table 23-3 Packet Filter Commands 23-5
Table 23-4 IP Source Guard Commands 23-11
Table 23-5 DHCP Snooping Commands 23-17

Downloaded from www.Manualslib.com manuals search engine

Table 24-1 Access Control List Commands 24-1
Table 24-2 IP ACL Commands 24-2
Table 24-3 MAC ACL Commands 24-16
Table 24-4 ACL Information Commands 24-26
Table 25-1 Interface Commands 25-1
Table 25-2 show interfaces switchport - display description 25-17
Table 26-1 Link Aggregation Commands 26-1
Table 26-2 show lacp counters - display description 26-11
Table 26-3 show lacp internal - display description 26-11
Table 26-4 show lacp neighbors - display description 26-13
Table 26-5 show lacp sysid - display description 26-14
Table 27-1 Mirror Port Commands 27-1
Table 28-1 Rate Limit Commands 28-1
Table 29-1 VDSL Commands 29-1
Table 29-2 Long-Reach Ethernet Commands 29-2
Table 29-3 VDSL2 Band Plans 29-5
Table 29-4 HAM Band Notches 29-7
Table 29-5 HAM Band Notches for Usage Types 29-10
Table 29-6 PSD Mask Options 29-17
Table 29-7 Line Profile Commands 29-35
Table 29-8 Alarm Profile Commands 29-51
Table 29-9 Commands for Displaying VDSL Information 29-61
Table 29-10 show lre - display description 29-79
Table 29-11 show lre phys-info - display description 29-81
Table 29-12 show lre rate-info - display description 29-82
Table 29-13 show lre phys-info - display description 29-83
Table 29-14 CPE Configuration Commands 29-86
Table 29-15 show cpe-info - display description 29-92
Table 30-1 Address Table Commands 30-1
Table 31-1 Spanning Tree Commands 31-1
Table 31-2 Recommended STA Path Cost Range 31-16
Table 31-3 Recommended STA Path Cost 31-16
Table 31-4 Default STA Path Costs 31-17
Table 32-1 VLAN Commands 32-1
Table 32-2 GVRP and Bridge Extension Commands 32-2
Table 32-3 Commands for Editing VLAN Groups 32-7
Table 32-4 Commands for Configuring VLAN Interfaces 32-9

Downloaded from www.Manualslib.com manuals search engine

Table 32-5 Commands for Displaying VLAN Information 32-16
Table 32-6 Private VLAN Commands 32-17
Table 32-7 Protocol-based VLAN Commands 32-20
Table 32-8 IEEE 802.1Q Tunneling Commands 32-25
Table 32-9 VLAN Swapping Commands 32-30
Table 33-1 Priority Commands 33-1
Table 33-2 Priority Commands (Layer 2) 33-1
Table 33-3 Default CoS Priority Levels 33-8
Table 33-4 Priority Commands (Layer 3 and 4) 33-11
Table 33-5 Mapping IP Precedence to CoS Values 33-14
Table 33-6 Mapping IP DSCP to CoS Values 33-16
Table 34-1 Quality of Service Commands 34-1
Table 35-1 Multicast Filtering Commands 35-1
Table 35-2 IGMP Snooping Commands 35-2
Table 35-3 IGMP Query Commands 35-7
Table 35-4 Static Multicast Routing Commands 35-12
Table 35-5 IGMP Filtering and Throttling Commands 35-14
Table 35-6 Multicast VLAN Registration Commands 35-23
Table 35-7 show mvr - display description 35-30
Table 35-8 show mvr interface - display description 35-31
Table 35-9 show mvr members - display description 35-32
Table 36-1 DNS Commands 36-1
Table 36-2 show dns cache - display description 36-10
Table 37-1 DHCP Commands 37-1
Table 37-2 DHCP Client Commands 37-1
Table 37-3 DHCP Relay Commands 37-2
Table 37-4 Inserting Option 82 Information 37-5
Table 38-1 Basic IP Configuration Commands 38-1
Table B-1 Troubleshooting Chart B-1

Downloaded from www.Manualslib.com manuals search engine

FIGURES

Figure 3-1 Home Page 3-3
Figure 3-2 Front Panel Indicators 3-4
Figure 4-1 System Information 4-2
Figure 4-2 System Health Information 4-5
Figure 4-3 Switch Information 4-8
Figure 4-4 Displaying Bridge Extension Configuration 4-10
Figure 4-5 IP Interface Configuration - Manual 4-12
Figure 4-6 IP Interface Configuration - DHCP 4-14
Figure 4-7 Configuring Support for Jumbo Frames 4-16
Figure 4-8 Copy Firmware 4-18
Figure 4-9 Setting the Startup Code 4-19
Figure 4-10 Deleting Files 4-19
Figure 4-11 Downloading Configuration Settings for Start-Up 4-22
Figure 4-12 Setting the Startup Configuration Settings 4-23
Figure 4-13 Configuring the Console Port 4-25
Figure 4-14 Configuring the Telnet Interface 4-28
Figure 4-15 System Logs 4-30
Figure 4-16 Remote Logs 4-32
Figure 4-17 Displaying Logs 4-33
Figure 4-18 Enabling and Configuring SMTP Alerts 4-35
Figure 4-19 Resetting the System 4-36
Figure 4-20 SNTP Configuration 4-38
Figure 4-21 Clock Time Zone 4-39
Figure 5-1 Enabling the SNMP Agent 5-4
Figure 5-2 Configuring SNMP Community Strings 5-5
Figure 5-3 Configuring SNMP Trap Managers 5-9
Figure 5-4 Setting the SNMPv3 Engine ID 5-11
Figure 5-5 Setting an Engine ID 5-12
Figure 5-6 Configuring SNMPv3 Users 5-14
Figure 5-7 Configuring Remote SNMPv3 Users 5-17
Figure 5-8 Configuring SNMPv3 Groups 5-23
Figure 5-9 Configuring SNMPv3 Views 5-25
Figure 6-1 User Accounts 6-2
Figure 6-2 Authentication Server Settings 6-6
Figure 6-3 HTTPS Settings 6-8
Figure 6-4 SSH Host-Key Settings 6-15

Downloaded from www.Manualslib.com manuals search engine

Figure 6-5 SSH Server Settings 6-17
Figure 6-6 802.1X Global Information 6-21
Figure 6-7 802.1X Global Configuration 6-22
Figure 6-8 802.1X Port Configuration 6-24
Figure 6-9 802.1X Port Statistics 6-27
Figure 6-10 IP Filter 6-29
Figure 7-1 Port Security 7-4
Figure 7-2 IP Source Guard Binding 7-7
Figure 7-3 DHCP Snooping Configuration 7-12
Figure 7-4 DHCP Snooping Information 7-14
Figure 7-5 Packet Filtering – Base Filter 7-18
Figure 7-6 Packet Filtering – IP/MAC Filter 7-19
Figure 8-1 Selecting ACL Type 8-4
Figure 8-2 ACL Configuration - Standard IP 8-5
Figure 8-3 ACL Configuration - Extended IP 8-7
Figure 8-4 ACL Configuration - MAC 8-9
Figure 8-5 Selecting ACL Mask Types 8-11
Figure 8-6 ACL Mask Configuration - IP 8-13
Figure 8-7 ACL Mask Configuration - MAC 8-15
Figure 8-8 ACL Port Binding 8-17
Figure 9-1 Port - Port Information 9-2
Figure 9-2 Port - Port Configuration 9-7
Figure 9-3 Static Trunk Configuration 9-10
Figure 9-4 LACP Trunk Configuration 9-12
Figure 9-5 LACP - Aggregation Port 9-15
Figure 9-6 LACP - Port Counters Information 9-17
Figure 9-7 LACP - Port Internal Information 9-20
Figure 9-8 LACP - Port Neighbors Information 9-22
Figure 9-9 Port Broadcast Control 9-24
Figure 9-10 Mirror Port Configuration 9-26
Figure 9-11 Rate Limit Configuration for Ethernet Interface 9-27
Figure 9-12 Rate Limit Configuration for VLAN Port Member . . . 9-28
Figure 9-13 Port Statistics 9-34
Figure 10-1 VDSL Global Configuration 10-6
Figure 10-2 VDSL Port Configuration 10-15
Figure 10-3 Line Profile Configuration 10-20
Figure 10-4 VDSL Status Information 10-23

Downloaded from www.Manualslib.com manuals search engine

Figure 10-5 VDSL Performance Statistics 10-28
Figure 10-6 Alarm Profile Configuration 10-35
Figure 10-7 CPE Information 10-39
Figure 10-8 CPE Information 10-43
Figure 11-1 Static Addresses 11-2
Figure 11-2 Dynamic Addresses 11-3
Figure 11-3 Address Aging 11-4
Figure 12-1 STA Information 12-6
Figure 12-2 STA Global Configuration 12-12
Figure 12-3 STA Port Information 12-16
Figure 12-4 STA Port Configuration 12-21
Figure 12-5 MSTP VLAN Configuration 12-23
Figure 12-6 MSTP Port Information 12-25
Figure 12-7 MSTP Port Configuration 12-29
Figure 13-1 Selecting the System Mode 13-2
Figure 13-2 Globally Enabling GVRP 13-6
Figure 13-3 VLAN Basic Information 13-7
Figure 13-4 VLAN Current Table 13-9
Figure 13-5 VLAN Static List - Creating VLANs 13-11
Figure 13-6 VLAN Static Table - Adding Static Members 13-13
Figure 13-7 VLAN Static Membership by Port 13-14
Figure 13-8 VLAN Port Configuration 13-17
Figure 13-9 Private VLAN Status 13-18
Figure 13-10 Private VLAN Link Status 13-19
Figure 13-11 Protocol VLAN Configuration 13-21
Figure 13-12 Protocol VLAN Port Configuration 13-23
Figure 13-13 Tunnel Port Configuration 13-31
Figure 13-14 VLAN Swap Configuration 13-34
Figure 14-1 Default Port Priority 14-2
Figure 14-2 Traffic Classes 14-5
Figure 14-3 Queue Mode 14-7
Figure 14-4 Queue Scheduling 14-8
Figure 14-5 IP Precedence/DSCP Priority Status 14-10
Figure 14-6 IP Precedence Priority 14-12
Figure 14-7 IP DSCP Priority 14-14
Figure 14-8 IP Port Priority Status 14-15
Figure 14-9 IP Port Priority Status 14-16

Downloaded from www.Manualslib.com manuals search engine

Figure 14-10 IP Port Priority 14-17
Figure 15-1 Configuring Class Maps 15-5
Figure 15-2 Configuring Policy Maps 15-9
Figure 15-3 Service Policy Settings 15-11
Figure 16-1 IGMP Configuration 16-6
Figure 16-2 Multicast Router Port Information 16-7
Figure 16-3 Static Multicast Router Port Configuration 16-8
Figure 16-4 IP Multicast Registration Table 16-10
Figure 16-5 IGMP Member Port Table 16-12
Figure 16-6 IGMP Immediate Leave Table 16-14
Figure 16-7 Enabling IGMP Filtering and Throttling 16-15
Figure 16-8 IGMP Profile Configuration 16-17
Figure 16-9 IGMP Filter and Throttling Port Configuration 16-19
Figure 16-10 MVR Global Configuration 16-23
Figure 16-11 MVR Port Information 16-24
Figure 16-12 MVR Port Configuration 16-28
Figure 16-13 MVR Group IP Information 16-29
Figure 16-14 MVR Group Member Configuration 16-31
Figure 17-1 DNS General Configuration 17-3
Figure 17-2 DNS Static Host Table 17-5
Figure 17-3 DNS Cache 17-7

Downloaded from www.Manualslib.com manuals search engine

SECTION I
GETTING STARTED

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

Introduction 1-1
Initial Configuration 2-1

Downloaded from www.Manualslib.com manuals search engine

GETTING STARTED

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 1
INTRODUCTION

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

The switch uses six frequency bands (three downstream and three upstream) for VDSL lines. These frequency bands conform to ITU-T G993.2 Annex C. Details of the frequency bands are given in the table below.

Key Features

Table 1-1 Key Features

Feature	Description
6-Band VDSL2	Total Bandwidth: 30 MHz Bandwidth Allocation: • Downstream (0.9-3.75, 5.2-8.5, 12-18.1 MHz) • Upstream (3.75-5.2, 8.5-12, 18.1-30 MHz)
Configuration Backup and Restore	Backup to TFTP server

Downloaded from www.Manualslib.com manuals search engine

Table 1-1 Key Features (Continued)

Feature	Description
User Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS Telnet – SSH SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X
Client Security	Private VLANs, IEEE 802.1X, MAC address filtering, IP/MAC address pair filtering, NetBIOS filtering, DHCP request/reply filtering
Access Control Lists	VDSL ports - 173 rules, 7 masks shared by 8-port groups Gigabit Ethernet ports - 52 rules, 7 masks
DHCP Client	Supported
DNS	Proxy service
Port Configuration	Speed and duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One port mirrored to single analysis port
Port Trunking	Supports up to 12 trunks using either static or dynamic trunking (LACP)
Storm Control	Broadcast, multicast and unknown unicast storm control
Address Table	Up to 16K MAC addresses in the forwarding table, 1024 static MAC addresses
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 256 using IEEE 802.1Q, port-based, protocol-based, private VLANs, and QinQ tunneling

Downloaded from www.Manualslib.com manuals search engine

Table 1-1 Key Features (Continued)

Feature	Description
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
Qualify of Service	Supports Differentiated Services (DiffServ)
Multicast Filtering	Supports IGMP snooping, query, profile filtering, and Multicast VLAN Registration
Tunneling	Supports IEEE 802.1Q tunneling (QinQ)

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Storm suppression prevents broadcast, multicast and unknown unicast traffic storms from engulfing the network. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication

Downloaded from www.Manualslib.com manuals search engine

server to verify the client's right to access the network via an authentication server (i.e., RADIUS server).

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

Port Configuration – You can manually configure the speed and duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Downloaded from www.Manualslib.com manuals search engine

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3-2002 (formerly IEEE 802.3ad) Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 12 trunks.

Storm Control – Broadcast, multicast and unknown unicast storm suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 0.75 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Downloaded from www.Manualslib.com manuals search engine

Spanning Tree Algorithm – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.

Downloaded from www.Manualslib.com manuals search engine

- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using eight priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Quality of Service – Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

Downloaded from www.Manualslib.com manuals search engine

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP snooping or query to manage multicast group registration; and multicast profile filtering to control access to specific multicast services. It also supports Multicast VLAN Registration (MVR) which allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, while preserving security and data isolation for normal traffic.

IEEE 802.1Q Tunneling (QinQ) – This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

Downloaded from www.Manualslib.com manuals search engine

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 4-20).

The following table lists some of the basic system defaults.

Table 1-2 System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	auto
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled

Downloaded from www.Manualslib.com manuals search engine

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Storm Protection	Status	Broadcast: enabled (all ports) Multicast: disabled Unknown unicast: disabled
	Rate Limit	Broadcast: 500 packets per second
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds

Downloaded from www.Manualslib.com manuals search engine

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
	QinQ Tunneling	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled
	DNS	Service: Disabled
	BOOTP	Disabled

Downloaded from www.Manualslib.com manuals search engine

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Disabled
	IGMP Filtering/Throttling	Disabled
	Multicast VLAN Registration	Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 2
INITIAL CONFIGURATION

Connecting to the Switch

Configuration Options

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: An IP address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address" on page 2-6.

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet or Secure Shell (SSH) connection over the network.

The switch's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as SMC EliteView.

Downloaded from www.Manualslib.com manuals search engine

The switch's web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 12 static or LACP trunks
- Enable port mirroring
- Set broadcast, multicast or unknown unicast storm control on any port
- Display system information and statistics

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

Downloaded from www.Manualslib.com manuals search engine

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set to any of the following baud rates: 9600, 19200, 38400, 57600, 115200 (Note: Set to 9600 baud if want to view all the system initialization messages.).
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

Notes: **1.** When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

2. Refer to "Line Commands" on page 20-26 for a complete description of console configuration options.

3. Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 18-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 18-12.

Downloaded from www.Manualslib.com manuals search engine

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

An IP address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-6.

Note: This switch supports four concurrent Telnet/SSH sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Downloaded from www.Manualslib.com manuals search engine

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.
2. At the Username prompt, enter "admin."
3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the "username" command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level.
2. Type "configure" and press <Enter>.
3. Type "username guest password 0 *password*," for the Normal Exec level, where *password* is your new password. Press <Enter>.

Downloaded from www.Manualslib.com manuals search engine

4. Type "username admin password 0 *password*," for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

      CLI session with the SMC7816M/VSW is opened.
      To end the CLI session, enter [Exit].

Console#configure                                              19-3
Console(config)#username guest password 0 [password]          22-2
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. The switch can be managed through Gigabit Ethernet uplink Ports 17 or 18 within the data network, or through Fast Ethernet Port 19 which is designed to serve as a dedicated management port outside of the data network.

All ports are all configured as members of VLAN 1 by default. To manage the switch through uplink ports 17 or 18, configure an IP address for the VLAN to which these ports are assigned. To manage the switch through the dedicated management port (Port 19), first assign this port to another VLAN outside of the data network, and then configure an IP address for management access to this VLAN.

You could also retain the uplink ports as members of the data network (i.e., the VLAN containing both the downlink and uplink ports), and add them as members to a separate network configured with an IP address for management access. Logically, the management VLAN should also contain the dedicated management port. Just note that no traffic is allowed to pass between any of the data ports 1-18 and the dedicated management port, regardless of the VLANs to which they are assigned. Port 19 is only provided for configuring and monitoring the switch.

Downloaded from www.Manualslib.com manuals search engine

Using the dedicated management port provides a back channel for troubleshooting when the switch cannot be reached through the data network. To provide additional security against eavesdropping on management traffic, leave the IP address for the data network (i.e., the VLAN containing ports 1-18) unconfigured.

To create a new VLAN and assign the management port to it, enter commands similar to those shown below:

1. From the Global Configuration mode prompt, type "vlan database" to access the vlan-configuration mode. Press <Enter>.
2. Enter "vlan *vlan-id* media ethernet state active" where "vlan-id" should be set to a VLAN index that does not contain the data ports.
3. Enter "vlan *vlan-id* name *vlan-name*" where "vlan-id" is the index for the management VLAN and "vlan-name" is a name chosen to represent the management VLAN.
4. Return to the Global Configuration mode by entering the "exit" command.
5. At the Global Configuration mode prompt, type "interface ethernet 1/19" to access the interface-configuration mode for Port 19. Press <Enter>.
6. Enter "switchport allowed vlan add 2 untagged" to add Port 19 as an untagged member of VLAN 2.
7. Enter "switchport native vlan 2" to configure the default VLAN ID for this port as VLAN 2. The default VLAN ID for all ports is VLAN 1, and this must be reassigned to another VLAN before you can remove Port 19 from VLAN 1 as shown in the next step.
8. Enter "switchport allowed vlan remove 1" to remove Port 19 from the data network.

Downloaded from www.Manualslib.com manuals search engine

9. Then follow the steps indicated in the next section to assign an IP address to this VLAN using manual configuration or automatic configuration via DHCP or BOOTP.

```
Console(config)#vlan database                                    32-7
Console(config-vlan)#vlan 2 name management media ethernet      32-8
Console(config-vlan)#exit
Console(config)#interface ethernet 1/19                          25-2
Console(config-if)#switchport allowed vlan add 2 untagged      32-14
Console(config-if)#switchport native vlan 2                    32-13
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#
```

Note: If you put the uplink ports (Ports 17 and 18) in a separate management VLAN, do not change their default VLAN ID. Nor should you remove these ports from the VLAN used for the data network. All data ports, both uplink and downlink, should be included in the same VLAN for normal operations (i.e., VLAN 1 by default).

You can configure an IP address in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: An IP address for this switch is obtained via DHCP by default.

Downloaded from www.Manualslib.com manuals search engine

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Network mask for this network
- Default gateway for the network

To assign an IP address to the switch, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address *ip-address netmask*," where "ip-address" is the switch IP address and "netmask" is the network mask for the network. Press <Enter>.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway *gateway*," where "gateway" is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 2                              25-2
Console(config-if)#ip address 192.168.1.5 255.255.255.0       38-2
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254              38-3
Console(config)#
```

Dynamic Configuration

If you select the "bootp" or "dhcp" option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to reset the switch start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the "bootp" or "dhcp" option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

Downloaded from www.Manualslib.com manuals search engine

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
   - To obtain IP settings via DHCP, type "ip address dhcp" and press <Enter>.
   - To obtain IP settings via BOOTP, type "ip address bootp" and press <Enter>.
3. Type "end" to return to the Privileged Exec mode. Press <Enter>.
4. Reset the switch by entering the "reload" command.
5. Wait a few minutes for the switch to reboot, and then check the IP configuration settings by typing the "show ip interface" command. Press <Enter>.
6. Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 2                                  25-2
Console(config-if)#ip address dhcp                                38-2
Console(config-if)#end
Console#reload                                                    19-5
:
Console#show ip interface                                         38-4
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP
Console#copy running-config startup-config                      20-17
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```


Downloaded from www.Manualslib.com manuals search engine

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default "public" community string that provides read access to the entire MIB tree, and a default view for the "private" community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see page 5-24).

Community Strings (for SNMP version 1 and 2c clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Downloaded from www.Manualslib.com manuals search engine

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server community *string mode*," where "string" is the community access string and "mode" is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type "no snmp-server community *string*," where "string" is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw            21-4
Console(config)#snmp-server community private
Console(config)#
```

Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the "snmp-server host" command. From the Privileged Exec level global configuration mode prompt, type:

"snmp-server host *host-address community-string*
[version {1 | 2c | 3 {auth | noauth | priv}}]"

where "host-address" is the IP address for the trap receiver, "community-string" specifies access rights for a version 1/2c host, or is the user name of a version 3 host, "version" indicates the SNMP client version, and "auth | noauth | priv" means that authentication, no authentication, or authentication and privacy is used for v3 clients.

Downloaded from www.Manualslib.com manuals search engine

Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host" on page 21-6. The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman           21-6
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called "mib-2" that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call "r&d" and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password "greenpeace" for authentication, and the password "einstien" for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included  21-13
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d   21-15
Console(config)#snmp-server user steve group r&d v3 auth md5
 greenpeace priv des56 einstien                              21-18
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to "Simple Network Management Protocol" on page 5-1, or refer to the specific CLI commands for SNMP starting on page 21-1.

Downloaded from www.Manualslib.com manuals search engine

Managing System Files

The switch's flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. The file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the master unit will also create a file named "startup1.cfg" that contains system settings for initialization, including information about the unit identifier, MAC address, and installed module type. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See "Saving or Restoring Configuration Settings" on page 4-20 for more information.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See "Managing Firmware" on page 4-17 for more information.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 32 Mbytes of flash memory for system files.

Downloaded from www.Manualslib.com manuals search engine

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the "copy" command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

There can be more than one user-defined configuration file saved in the switch's flash memory, but only one is designated as the "startup" file that is loaded when the switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config:**<*filename*> command.

The maximum number of saved configuration files depends on available flash memory, with each configuration file normally requiring less than 20 kbytes. The amount of available flash memory can be checked by using the **dir** command.

Downloaded from www.Manualslib.com manuals search engine

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config                    20-17
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```


Downloaded from www.Manualslib.com manuals search engine

SECTION II
SWITCH MANAGEMENT

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser, and a brief example for the Command Line Interface.

Configuring the Switch 3-1

Basic Management Tasks 4-1

Simple Network Management Protocol 5-1

User Authentication 6-1

Client Security 7-1

Access Control Lists 8-1

Port Configuration 9-1

VDSL Configuration 10-1

Address Table Settings 11-1

Spanning Tree Algorithm 12-1

VLAN Configuration 13-1

Class of Service 14-1

Quality of Service 15-1

Multicast Filtering 16-1

Domain Name Service 17-1

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 3
CONFIGURING THE SWITCH

Using the Web Interface

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 18 "Overview of the Command Line Interface."

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 2-6.)
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 2-5.)
3. After you enter a user name and password, you will have access to the system configuration program.

Downloaded from www.Manualslib.com manuals search engine

Notes: **1.** You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

2. If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings" on page 12-18.

Downloaded from www.Manualslib.com manuals search engine

Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password "admin" is used for the administrator.

Home Page

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

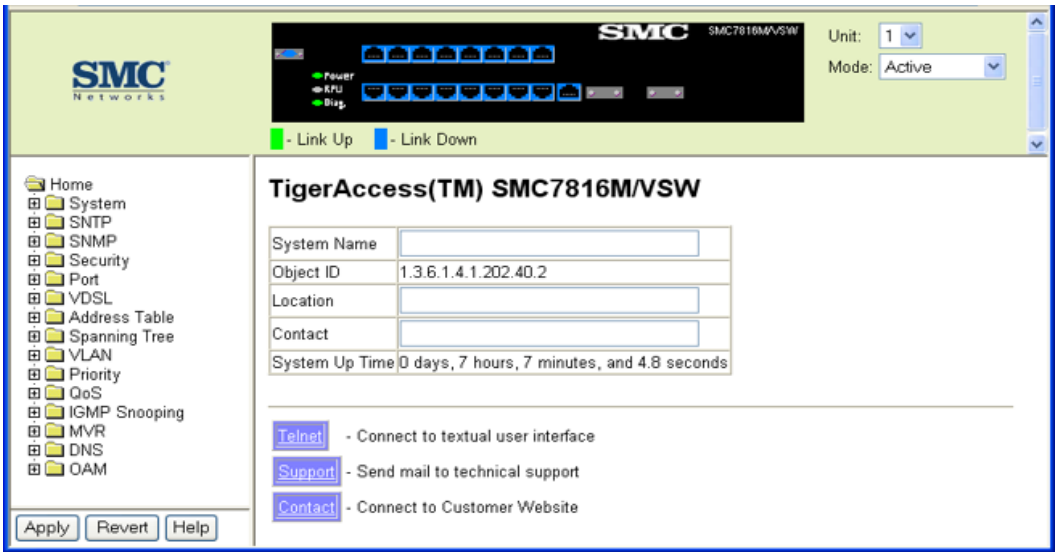


Figure 3-1 Home Page

Downloaded from www.Manualslib.com manuals search engine

Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

Table 3-1 Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
Help	Links directly to web help.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

Panel Display

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control). Clicking on the image of a port opens the Port Configuration page as described on page 9-4.

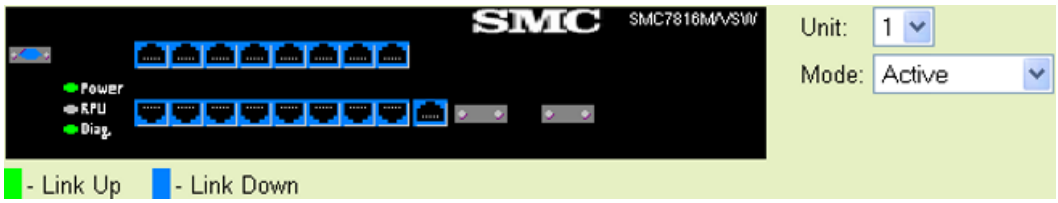


Figure 3-2 Front Panel Indicators

Downloaded from www.Manualslib.com manuals search engine

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 3-2 Switch Main Menu

Menu	Description	Page
System		4-1
System Information	Provides basic system description, including contact information	4-1
System Health	Shows status of fans, CPU and memory	4-4
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	4-7
Bridge Extension	Shows the bridge extension parameters	4-9
IP Configuration	Sets the IP address for management access	4-11
Jumbo Frames	Enables support for jumbo frames	4-16
File Management		4-17
Copy Operation	Allows the transfer and copying files	4-18
Delete	Allows deletion of files from the flash memory	4-18
Set Startup	Sets the startup file	4-18
Line		4-24
Console	Sets console port connection parameters	4-24
Telnet	Sets Telnet connection parameters	4-26
Log		4-29
Logs	Sends error messages to a logging process	4-33
System Logs	Stores and displays error messages	4-29
Remote Logs	Configures the logging of messages to a remote logging process	4-31
SMTP	Sends an SMTP client message to a participating server	4-34

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Reset	Restarts the switch	4-36
SNTP		4-37
Configuration	Configures SNTP client settings, including a specified list of servers	4-37
Clock Time Zone	Sets the local time zone for the system clock	4-39
SNMP		5-1
Configuration	Configures community strings and related trap functions	5-4
Agent Status	Enables or disables SNMP	5-4
SNMPv3		5-10
Engine ID	Sets the SNMP v3 engine ID	5-10
Remote Engine ID	Sets the SNMP v3 engine ID on a remote device	5-11
Users	Configures SNMP v3 users	5-12
Remote Users	Configures SNMP v3 users on a remote device	5-15
Groups	Configures SNMP v3 groups	5-18
Views	Configures SNMP v3 views	5-24
Security		6-1
User Accounts	Configures user names, passwords, and access levels	6-1
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	6-3
HTTPS Settings	Configures secure HTTP settings	6-7
SSH		6-10
Settings	Configures Secure Shell server settings	6-16
Host-Key Settings	Generates the host key pair (public and private)	6-13
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	7-2

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
802.1X	Port authentication	6-19
Information	Displays global configuration settings	6-21
Configuration	Configures global configuration parameters	6-22
Port Configuration	Sets the authentication mode for individual ports	6-23
Statistics	Displays protocol statistics for the selected port	6-26
ACL		8-1
Configuration	Configures packet filtering based on IP or MAC addresses	8-1
Mask Configuration	Controls the order in which ACL rules are checked	8-10
Port Binding	Binds a port to the specified ACL	8-16
IP Filter	Configures IP addresses that are allowed management access	6-28
DHCP Snooping		7-8
Configuration	Configures DHCP snooping globally or for specific VLANs, MAC address verification, and trusted ports	7-8
Information	Shows configured settings, trusted ports, and binding table entries	7-13
IP Source Guard		7-5
Configuration	Filters IP traffic on unsecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings	7-5
Packet Filter		7-15
Base Filter	Filters DHCP request packets, DHCP reply packets, or NetBIOS packets	7-15
IP/MAC Filter	Filters IP/MAC address pairs	7-18
Port		9-1
Port Information	Displays port connection status	9-1
Trunk Information	Displays trunk connection status	9-1
Port Configuration	Configures port connection settings	9-4

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Trunk Configuration	Configures trunk connection settings	9-4
Trunk Membership	Specifies ports to group into static trunks	9-9
LACP		9-11
Configuration	Allows ports to dynamically join trunks	9-11
Aggregation Port	Configures parameters for link aggregation group members	9-13
Port Counters Information	Displays statistics for LACP protocol messages	9-17
Port Internal Information	Displays settings and operational state for the local side	9-18
Port Neighbors Information	Displays settings and operational state for the remote side	9-21
Port Broadcast Control	Sets the broadcast storm threshold for each port	9-23
Trunk Broadcast Control	Sets the broadcast storm threshold for each trunk	9-23
Mirror Port Configuration	Sets the source and target ports for mirroring	9-25
Rate Limit		9-26
Input Port Configuration	Sets the input rate limit for each port	9-26
Input Trunk Configuration	Sets the input rate limit for each trunk	9-26
Output Port Configuration	Sets the output rate limit for each port	9-26
Output Trunk Configuration	Sets the output rate limit for each trunk	9-26
Input VLAN Configuration	Sets the input rate limit member port of specified VLAN	9-26
Port Statistics	Lists Ethernet and RMON port statistics	9-29

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
VDSL		10-1
Global Configuration	Configures global VDSL variables which can be applied to all ports	10-1
VDSL Port Configuration	Configures communication parameters for VDSL ports	10-7
Line Profile Configuration	Configures a list of communication parameters which can be applied to all VDSL ports or to a selected group of ports	10-16
VDSL Status Information	Displays information on VDSL configuration settings, signal status, and communication statistics	10-21
VDSL Performance Statistics	Displays performance information including common error conditions over predefined intervals for the VDSL line, as well as statistics for Ethernet traffic and High-Level.Data-Link Control (HDLC)	10-25
Alarm Profile Configuration	Configures a list of threshold values for error states which can be applied a selected group of VDSL ports	10-30
CPE Information	Displays information on CPE software module versions, buffer status and version, and performance counters	10-36
VDSL OAM	Controls various functions for VDSL chip on local switch port and for CPE, resetting the CPE, and upgrading firmware on CPE	10-41
Address Table		11-1
Static Addresses	Displays entries for interface, address or VLAN	11-1
Dynamic Addresses	Displays or edits static entries in the Address Table	11-2
Address Aging	Sets timeout for dynamically learned entries	11-4

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Spanning Tree		12-1
STA		
Information	Displays STA values used for the bridge	12-4
Configuration	Configures global bridge settings for STP, RSTP and MSTP	12-8
Port Information	Displays individual port settings for STA	12-13
Trunk Information	Displays individual trunk settings for STA	12-13
Port Configuration	Configures individual port settings for STA	12-18
Trunk Configuration	Configures individual trunk settings for STA	12-18
MSTP		
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	12-22
Port Information	Displays port settings for a specified MST instance	12-25
Trunk Information	Displays trunk settings for a specified MST instance	12-25
Port Configuration	Configures port settings for a specified MST instance	12-27
Trunk Configuration	Configures trunk settings for a specified MST instance	12-27
VLAN		13-1
System Mode	Configure the switch to operate in normal mode or one of the tunneling modes (QinQ or VLAN Swap)	13-1
802.1Q VLAN		13-2
GVRP Status	Enables GVRP VLAN registration protocol	13-6
Basic Information	Displays information on the VLAN type supported by this switch	13-7
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	13-8
Static List	Used to create or remove VLAN groups	13-10
Static Table	Modifies the settings for an existing VLAN	13-12

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden	13-14
Port Configuration	Specifies default PVID and VLAN attributes	13-15
Trunk Configuration	Specifies default trunk VID and VLAN attributes	13-15
Private VLAN		13-18
Status	Enables or disables the private VLAN	13-18
Link Status	Configures the private VLAN	13-19
Protocol VLAN		13-20
Configuration	Creates a protocol group, specifying the supported protocols	13-21
Port Configuration	Maps a protocol group to a VLAN	13-22
802.1Q Tunneling	Sets the Tag Protocol Identifier (TPID) and copying of the priority bits from inner to outer VLAN tag	13-24
VLAN Swap	Manually maps VLAN IDs between uplink and downlink ports for use in QinQ tunneling	13-33
Priority		14-1
Default Port Priority	Sets the default priority for each port	14-1
Default Trunk Priority	Sets the default priority for each trunk	14-1
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	14-3
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	14-6
Queue Scheduling	Configures Weighted Round Robin queueing	14-7
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	14-9
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	14-11
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	14-13

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
IPv6 Mapping	Assigns IPv6 traffic classes to one of the Class-of-Service values	14-15
IP Port Priority Status	Globally enables or disables IP Port Priority	14-16
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	14-11
QoS		15-1
DiffServ	Configure QoS classification criteria and service policies	15-2
Class Map	Creates a class map for a type of traffic	15-3
Policy Map	Creates a policy map for multiple interfaces	15-6
Service Policy	Applies a policy map defined to an ingress port	15-10
IGMP Snooping		16-2
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	16-4
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	16-7
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	16-8
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	16-9
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	16-9
IGMP Immediate Leave Table	Immediately deletes a member port of a multicast service if a leave packet is received	16-13
IGMP Filter Configuration	Enables IGMP filtering and creates profile groups	16-15
IGMP Profile Group Configuration	Sets IGMP filter profile groups and access mode	16-16
IGMP Filter/Throttling Port Configuration	Assigns IGMP filter profiles to port interfaces and sets throttle mode	16-18

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
IGMP Filter/Throttling Trunk Configuration	Assigns IGMP filter profiles to trunk interfaces and sets throttle mode	16-18
MVR		16-20
Configuration	Globally enables MVR, sets the MVR VLAN, adds multicast stream addresses	16-21
Port Information	Displays MVR interface type, MVR operational and activity status, and immediate leave status	16-24
Trunk Information	Displays MVR interface type, MVR operational and activity status, and immediate leave status	16-24
Group IP Information	Displays the ports attached to an MVR multicast stream	16-28
Port Configuration	Configures MVR interface type and immediate leave status	16-26
Trunk Configuration	Configures MVR interface type and immediate leave status	16-26
Group Member Configuration	Statically assigns MVR multicast streams to an interface	16-30
DNS		17-1
General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup	17-1
Static Host Table	Configures static entries for domain name to address mapping	17-4
Cache	Displays cache entries discovered by designated name servers	17-6

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 4
BASIC MANAGEMENT TASKS

This chapter describes the basic functions required to set up management access to the switch, display or upgrade operating software, or reset the system.

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **System Description** – Brief description of device type.
- **MAC Address** – The physical layer address for this switch.
- **Web Server** – Shows if management access via HTTP is enabled.
- **Web Server Port** – Shows the TCP port number used by the web interface.
- **Web Secure Server** – Shows if management access via HTTPS is enabled.

Downloaded from www.Manualslib.com manuals search engine

- **Web Secure Server Port** – Shows the TCP port used by the HTTPS interface.
- **Telnet Server** – Shows if management access via Telnet is enabled.
- **Telnet Server Port** – Shows the TCP port used by the Telnet interface.
- **Authentication Login** – Shows the user login authentication sequence.
- **Jumbo Frame** – Shows if jumbo frames are enabled.
- **POST Result** – Shows results of the power-on self-test
- **System Health** – Shows the functional status of key system components

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)

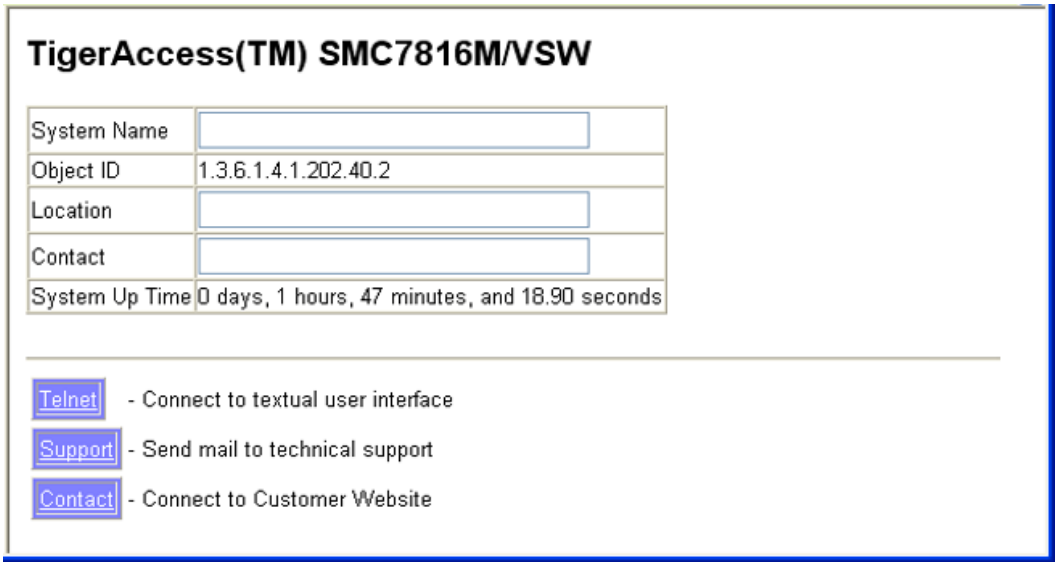


Figure 4-1 System Information

Downloaded from www.Manualslib.com manuals search engine

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname R&D 5                                    20-2
Console(config)#snmp-server location WC 9                         21-5
Console(config)#snmp-server contact Ted                           21-5
Console(config)#exit
Console#show system                                               20-8
System Description: TigerAccess(TM) SMC7816M/VSW
System OID String: 1.3.6.1.4.1.202.40.2
System Information
 System Up Time:          0 days, 1 hours, 56 minutes, and 9.89
seconds
 System Name:             R&D 5
 System Location:         WC 9
 System Contact:          Ted
 MAC Address (Unit1):     00-01-02-03-04-05
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled

 POST Result:
DUMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
PCI Device 1 Test ............ PASS
I2C Bus Initialization ....... PASS

Done All Pass.

SYSTEM health:
  PCI work OK
    PCI fail counter 0:
  I2C 0 work OK
    failed counter 0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying System Health

Use the System Health Information page to display the status of the fans, internal temperature, main board, CPU, and system memory.

Field Attributes

General Status

- **Fan Status** – The fan's functioning status.
- **Fan Failed Times** – The number of times the fan has failed since the system was booted.
- **Thermal Status** – The temperature status of the system. (Normal or Too High)
- **System Hardware Status** – The status of the overall system. (OK or Failed)

CPU Status

- **Current Utilization** – Current percentage of CPU utilization.
- **Max Utilization Statistically** – Maximum statistical utilization over the past 10 seconds.
- **Average Utilization Statistically** – Average statistical utilization since the system was booted.
- **Peak Time** – Time at which the CPU reach its peak utilization.
- **Peak Time Duration** – Duration of peak utilization.
- **Utilization Raising Alarm Threshold**[1] – Rising threshold for CPU utilization alarm. (Range: 1-100%; Default: 90%)
- **Utilization Falling Alarm Threshold**[1] – Falling threshold for CPU utilization alarm. (Range: 1-100%; Default: 90%)

Memory Status

- **Total Amount** – Total amount of memory provided by the system.
- **Allocated Amount** – Amount of memory allocated to active processes.

1. Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Downloaded from www.Manualslib.com manuals search engine

- **Free Amount** – Amount of memory currently free for use.
- **Freed / Total** – Percentage of free memory compared to total memory.
- **Utilization Raising Alarm Threshold**[1] – Rising threshold for memory utilization alarm. (Range: 1-100%; Default: 90%)
- **Utilization Falling Alarm Threshold**[1] – Falling threshold for memory utilization alarm. (Range: 1-100%; Default: 90%)

Web – Click System, System Health Information.

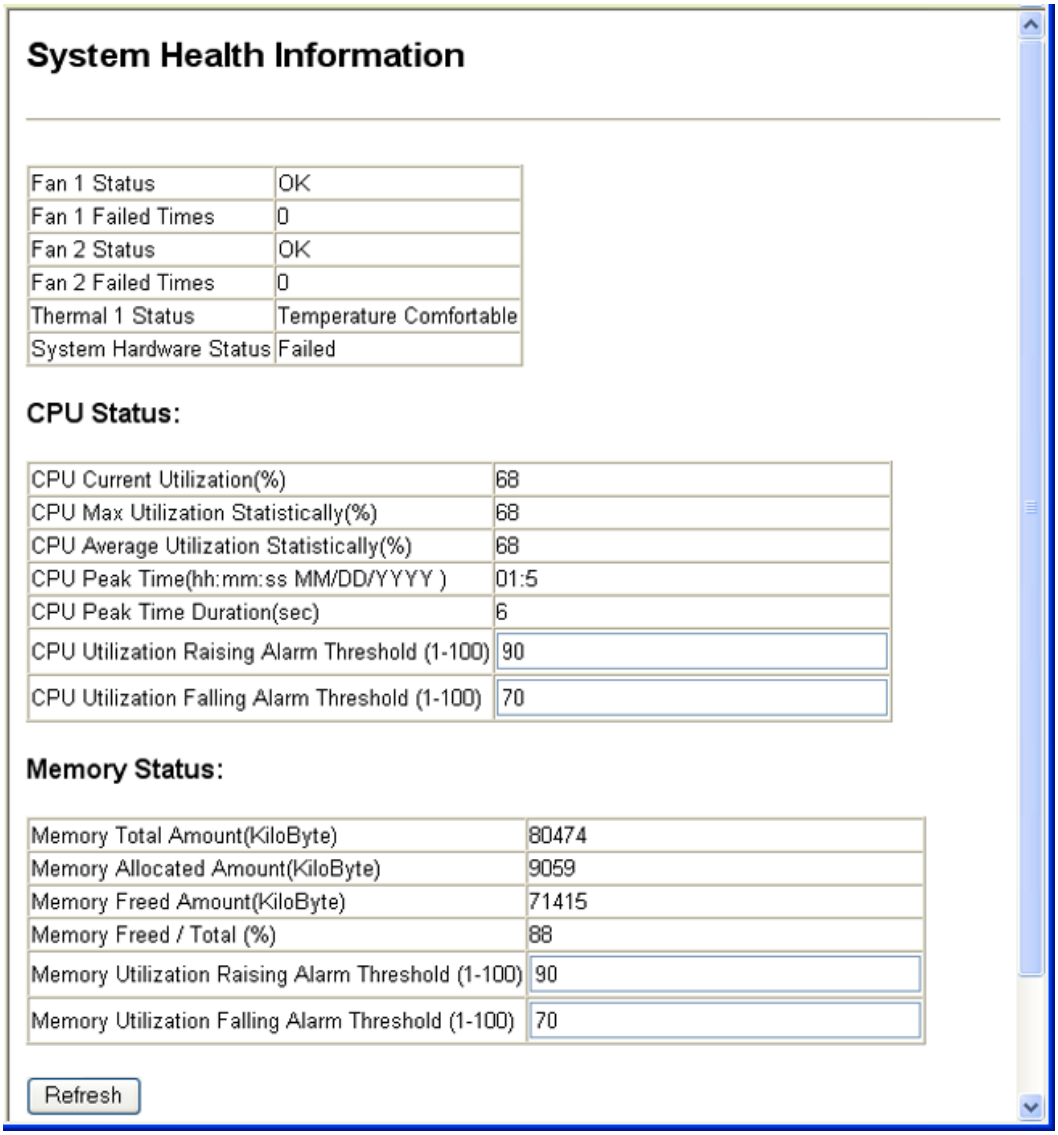

System Health Information
Fan 1 Status OK
Fan 1 Failed Times 0
Fan 2 Status OK
Fan 2 Failed Times 0
Thermal 1 Status Temperature Comfortable
System Hardware Status Failed
CPU Status:
CPU Current Utilization(%) 68
CPU Max Utilization Statistically(%) 68
CPU Average Utilization Statistically(%) 68
CPU Peak Time(hh:mm:ss MM/DD/YYYY) 01:5
CPU Peak Time Duration(sec) 6
CPU Utilization Raising Alarm Threshold (1-100) 90
CPU Utilization Falling Alarm Threshold (1-100) 70
Memory Status:
Memory Total Amount(KiloByte) 80474
Memory Allocated Amount(KiloByte) 9059
Memory Freed Amount(KiloByte) 71415
Memory Freed / Total (%) 88
Memory Utilization Raising Alarm Threshold (1-100) 90
Memory Utilization Falling Alarm Threshold (1-100) 70
Refresh

Figure 4-2 System Health Information

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the following commands to display the status of the CPU and system memory.

```
Console#show cpu utilization                                    20-11

 CPU current utilization  : 73%
     Max utilization in 10s: 73%
     Avg utilization in 10s: 73%

     peak utilization: 73%
     peak utilization begin : 02:33:50 01/01/2001
     peak utilization during: 10(s)

     utilization Raise  threshold: 90%
     utilization Falling threshold: 70%
Console#show memory status                                      20-12

FREE LIST:
  num     addr      size
  --- ---------- ----------
    1  0x7176640       1024
    2  0x7176498         56


SUMMARY:
 status   bytes    blocks   avg block  max block
 ------ --------- -------- ---------- ----------
current
   free      1080        2        540      1024
  alloc   8984600    46724        192         -
cumulative
  alloc  21630136   156917        137         -

Console#show system                                             20-8
.
.
.
SYSTEM health:
  Fan 1:
     Status:OK
     Fail times:0
  Fan 2:
     Status:OK
     Fail times:0
  Fan 3:
     Status:OK
     Fail times:0
  Thermal 1:
     Temperature Comfortable.
  PCI work OK
    PCI fail counter 0:
  I2C 0 work OK
    failed counter 0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – Serial number of main board.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.

Signal Board

- **Serial Number** – Serial number of VDSL2 signal processor board. This board includes the Burst Mode Engine (BME), Digital Signal Processing (DSP) engine, Analog Front End (AFE), and Integrated Front Ends (IFE) for 100/100 Mbps symmetric and 100/50 Mbps asymmetric line drivers.
- **Hardware Version** – Hardware version of VDSL2 signal processing board.

Management Software

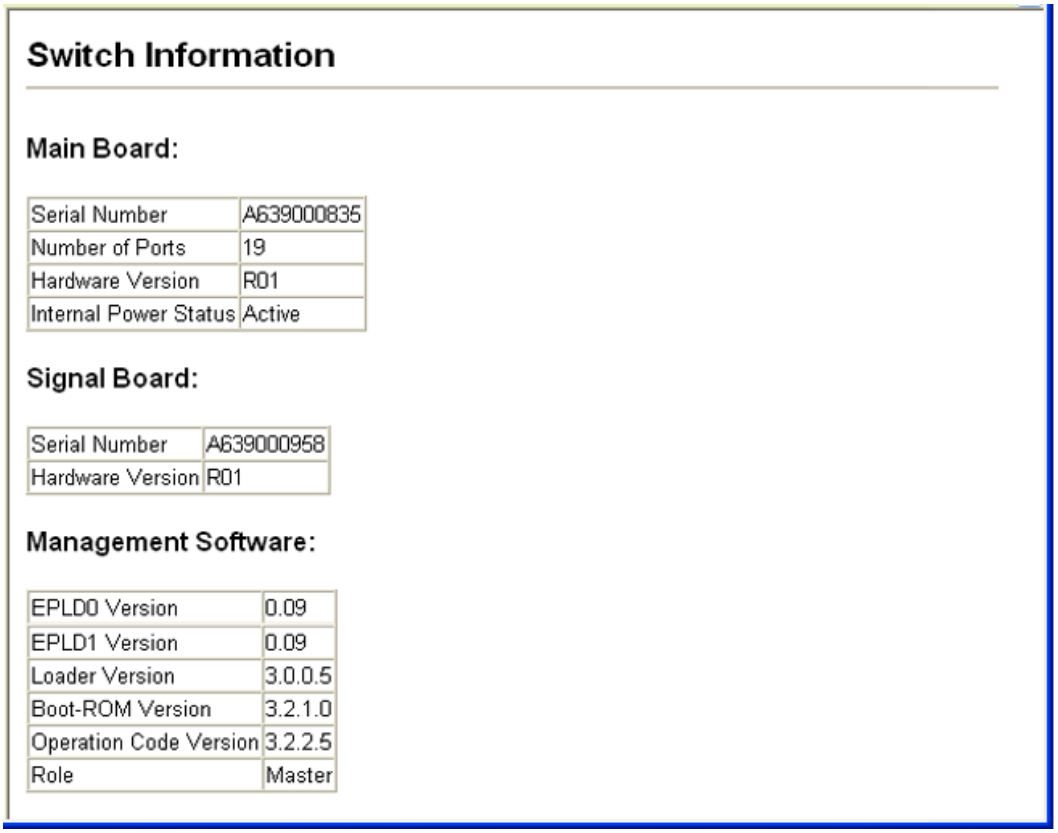
- **EPLD Version** – Version number of EEPROM Programmable Logic Devices.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., stacking not supported).

Downloaded from www.Manualslib.com manuals search engine

These additional parameters are displayed for the CLI.

- **Unit ID** – Unit number in stack.
- **BME firmware version** – Version number of Burst Mode Engine.

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	A639000835
Number of Ports	19
Hardware Version	R01
Internal Power Status	Active

Signal Board:

Serial Number	A639000958
Hardware Version	R01

Management Software:

EPLD0 Version	0.09
EPLD1 Version	0.09
Loader Version	3.0.0.5
Boot-ROM Version	3.2.1.0
Operation Code Version	3.2.2.5
Role	Master

Figure 4-3 Switch Information

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the following command to display version information.

```
Console#show version                                          20-10
Unit 1
 Mainboard Serial Number:              A639000835
 Signalboard Serial Number:            A639000958
 Mainboard Hardware Version:           R01
 Signalboard Hardware Version:         R01
 EPLD1 Version:                        0.09
 EPLD2 Version:                        0.09
 Number of Ports:                      19
 Main Power Status:                    Up

Agent (Master)
 Unit ID:                  1
 Loader Version:           3.0.0.5
 Boot ROM Version:         3.2.1.0
 Operation Code Version:   3.2.2.5

 Bme firmware version:     Firmware-VTU-O:1.0.5r11IK004010
Console#
```

Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service" on page 14-1.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 11-1.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.

Downloaded from www.Manualslib.com manuals search engine

- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 13-1.)
- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.

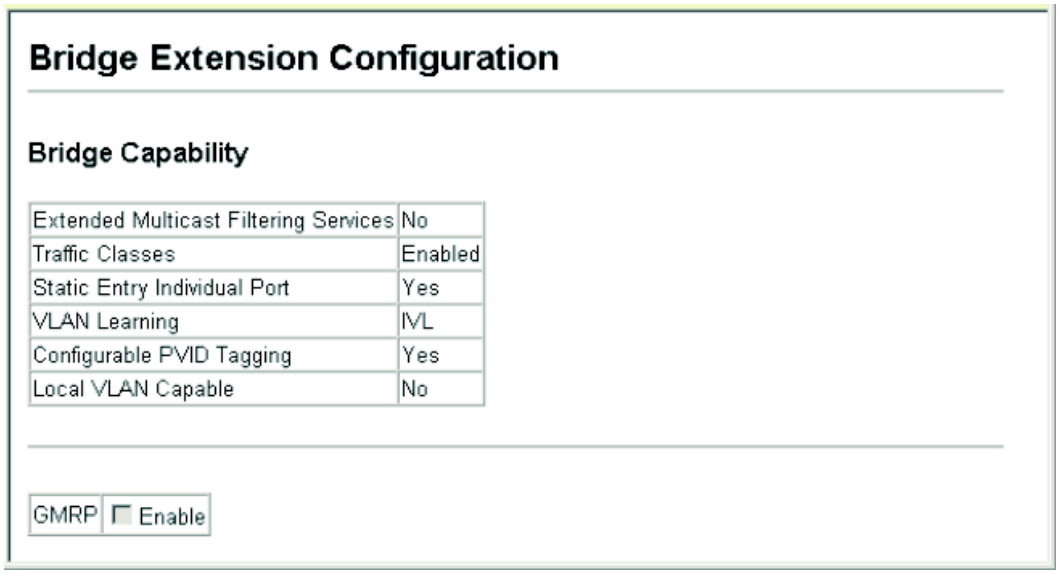


Figure 4-4 Displaying Bridge Extension Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – Enter the following command.

```
Console#show bridge-ext                                          32-3
 Max Support VLAN Numbers:              255
 Max Support VLAN ID:                   4094
 Extended Multicast Filtering Services: No
 Static Entry Individual Port:          Yes
 VLAN Learning:                         IVL
 Configurable PVID Tagging:             Yes
 Local VLAN Capable:                    No
 Traffic Classes:                       Enabled
 Global GVRP Status:                    Disabled
 GMRP:                                  Disabled
Console#
```

Setting the Switch's IP Address

This section describes how to configure an IP interface for management access over the network. The IP address for this switch is obtained via DHCP by default. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Attributes

- **Management VLAN** – ID of the configured VLAN (1-4094). By default, all ports on the switch are members of VLAN 1. However, the management station should only be attached to Ports 17-19 within any VLAN, as long as that VLAN has been assigned an IP address. Refer to "Setting an IP Address" on page 2-6 for a detailed description of setting the management VLAN and access port.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP

Downloaded from www.Manualslib.com manuals search engine

will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)

- **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Gateway IP Address** – IP address of the gateway router between the stack and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.

Manual Configuration

Web – Click System, IP Configuration. Select the VLAN through which the management station is attached. Enter the IP address, subnet mask and gateway, then click Apply.

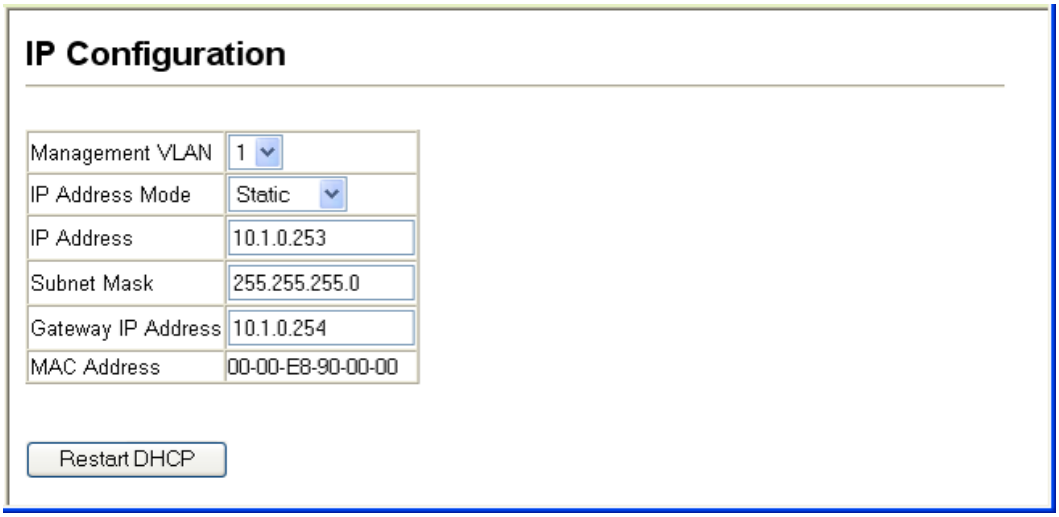


Figure 4-5 IP Interface Configuration - Manual

Downloaded from www.Manualslib.com manuals search engine

CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1                                    25-2
Console(config-if)#ip address 10.1.0.253 255.255.255.0              38-2
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                       38-3
Console(config)#end
Console#show ip interface                                           38-4
 IP Address and Netmask:  10.1.0.253 255.255.255.0 on VLAN 2,
 Address Mode:            User
Console#
```

This example first sets up a dedicated VLAN for management access. It adds Port 19 (the management port) to that VLAN and also removes this port from the VLAN 1, which is left for use by the data network. It then specifies the management interface, IP address and default gateway. For information on making these configuration changes through the web interface, refer to Chapter 13 "VLAN Configuration."

```
Console#config
Console(config)#vlan database                                       32-7
Console(config-vlan)#vlan 2 name management media ethernet          32-8
Console(config-vlan)#exit
Console(config)#interface ethernet 1/19                             25-2
Console(config-if)#switchport allowed vlan add 2                    32-14
Console(config-if)#switchport native vlan 2                         32-13
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport forbidden vlan add 1                  32-15
Console(config-if)#exit
Console(config)#interface vlan 2                                    25-2
Console(config-if)#ip address 10.1.0.253 255.255.255.0              38-2
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                       38-3
Console(config)#end
Console#show ip interface                                           38-4
 IP Address and Netmask:  10.1.0.253 255.255.255.0 on VLAN 2,
 Address Mode:            User
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP Configuration. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on each power reset.

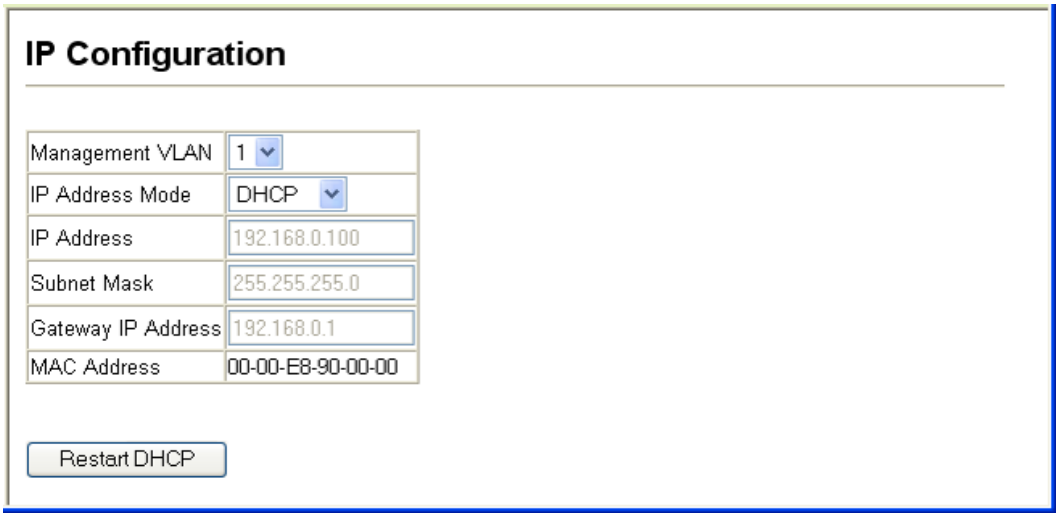


Figure 4-6 IP Interface Configuration - DHCP

Note: If you lose your management connection, make a console connection to the Master unit and enter "show ip interface" to determine the new stack address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the "ip dhcp restart" command.

```
Console#config
Console(config)#interface vlan 1                                    25-2
Console(config-if)#ip address dhcp                                  38-2
Console(config-if)#end
Console#ip dhcp restart                                             37-1
Console#show ip interface                                           38-4
 IP Address and Netmask:  192.168.0.100 255.255.255.0 on VLAN 1,
 Address Mode:            DHCP
Console#
```


Downloaded from www.Manualslib.com manuals search engine

This example first sets up a dedicated VLAN for management access. It adds Port 19 (the management port) to that VLAN and also removes this port from the VLAN 1, which is left for use by the data network. It then specifies the management interface, IP address and default gateway. For information on making these configuration changes through the web interface, refer to Chapter 13 "VLAN Configuration."

```
Console#config
Console(config)#vlan database                                    32-7
Console(config-vlan)#vlan 2 name management media ethernet       32-8
Console(config-vlan)#exit
Console(config)#interface ethernet 1/19                          25-2
Console(config-if)#switchport allowed vlan add 2                 32-14
Console(config-if)#switchport native vlan 2                      32-13
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport forbidden vlan add 1               32-15
Console(config-if)#exit
Console(config)#interface vlan 2                                 25-2
Console(config-if)#ip address dhcp                               38-2
Console(config-if)#end
Console#ip dhcp restart                                          37-1
Console#show ip interface                                        38-4
 IP Address and Netmask:  192.168.0.100 255.255.255.0 on VLAN 2,
 Address Mode:            DHCP
Console(config)#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the stack is moved to another network segment, you will lose management access to the stack. In this case, you can reboot the stack or submit a client request to restart DHCP service via the CLI.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                          37-1
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Support for Jumbo Frames

The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

Command Usage

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Command Attributes

Jumbo Packet Status – Configures support for jumbo frames. (Default: Disabled)

Web – Click System, Jumbo Frames. Enable or disable support for jumbo frames, and click Apply.

Figure 4-7 Configuring Support for Jumbo Frames

CLI – This example enables jumbo frames globally for the switch.

```
Console(config)#jumbo frame                                    20-15
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version. You must specify the method of file transfer, along with the file type and file names as required.

Command Attributes

- File Transfer Method – The firmware copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify opcode (operational code) to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloaded from www.Manualslib.com manuals search engine

Downloading System Software from a Server

When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, File Management, Copy Operation. Select "tftp to file" as the file transfer method, enter the IP address of the TFTP server, set the file type to "opcode," enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Apply. If you replaced the current firmware used for startup and want to start using the new operation code, reboot the system via the System/Reset menu.

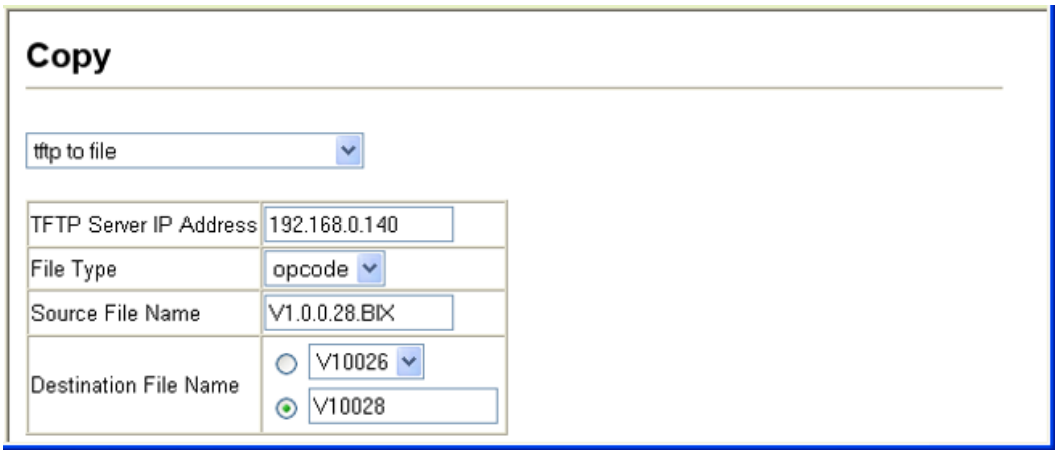


Figure 4-8 Copy Firmware

Downloaded from www.Manualslib.com manuals search engine

If you download to a new destination file, go to the File Management, Set Start-Up menu, mark the operation code file used at startup, and click Apply. To start the new firmware, reboot the system via the System/Reset menu.

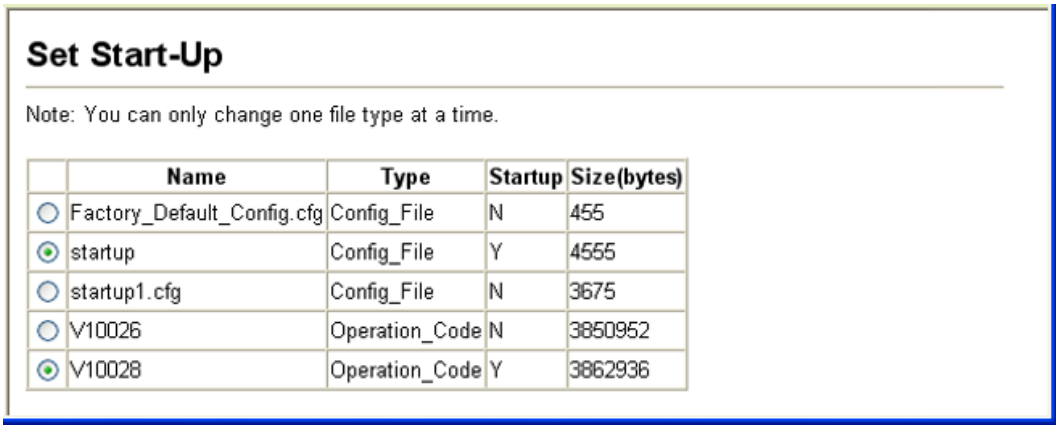


Figure 4-9 Setting the Startup Code

To delete a file select System, File Management, Delete. Select the file name from the given list by checking the tick box and click Apply. Note that the file currently designated as the startup code cannot be deleted.

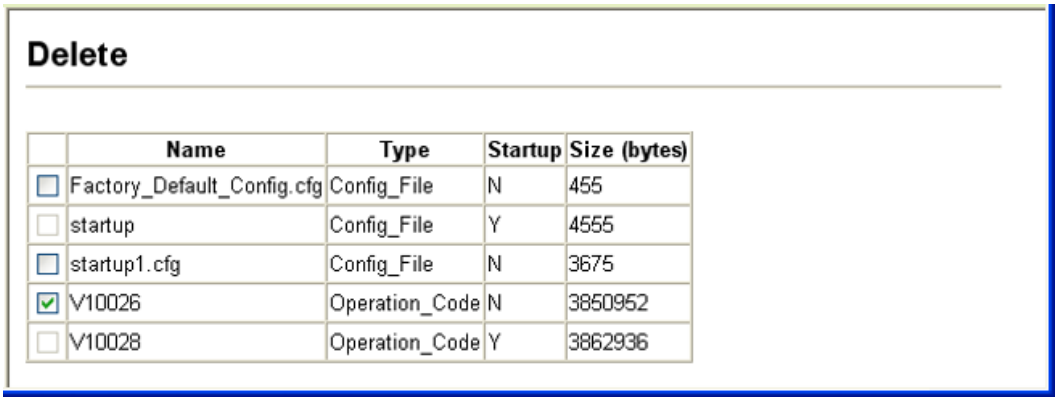


Figure 4-10 Deleting Files

CLI – To download new firmware form a TFTP server, enter the IP address of the TFTP server, select "config" as the file type, then enter the source and destination file names. When the file has finished downloading, set the new file to start up the system, and then restart the switch.

Downloaded from www.Manualslib.com manuals search engine

To start the new firmware, enter the "reload" command or reboot the system.

```
Console#copy tftp file                                          20-17
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: V3.1.16.20.bix
Destination file name: V311620
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V311620                      20-25
Console(config)#exit
Console#reload                                                  19-5
System will be restarted, continue <y/n>?
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server, or copy files to and from switch units in a stack. The configuration file can be later downloaded to restore the switch's settings.

Command Attributes

- File Transfer Method – The configuration copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to running-config – Copies a file in the switch to the running configuration.
  - file to startup-config – Copies a file in the switch to the startup configuration.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - partial-running-config to startup-config – Copies the IP address, subnet mask, default gateway, SNMP community strings, system user names and passwords to a configuration file. All other settings will be set to default values when the system is rebooted using this file.

Downloaded from www.Manualslib.com manuals search engine

  - running-config to file – Copies the running configuration to a file.
  - running-config to startup-config – Copies the running config to the startup config.
  - running-config to tftp – Copies the running configuration to a TFTP server.
  - startup-config to file – Copies the startup configuration to a file on the switch.
  - startup-config to running-config – Copies the startup config to the running config.
  - startup-config to tftp – Copies the startup configuration to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
  - tftp to running-config – Copies a file from a TFTP server to the running config.
  - tftp to startup-config – Copies a file from a TFTP server to the startup config.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify config (configuration) to copy configuration settings.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

Downloaded from www.Manualslib.com manuals search engine

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, File Management, Copy Operation. Choose "tftp to startup-config" or "tftp to file," and enter the IP address of the TFTP server. Specify the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Apply.

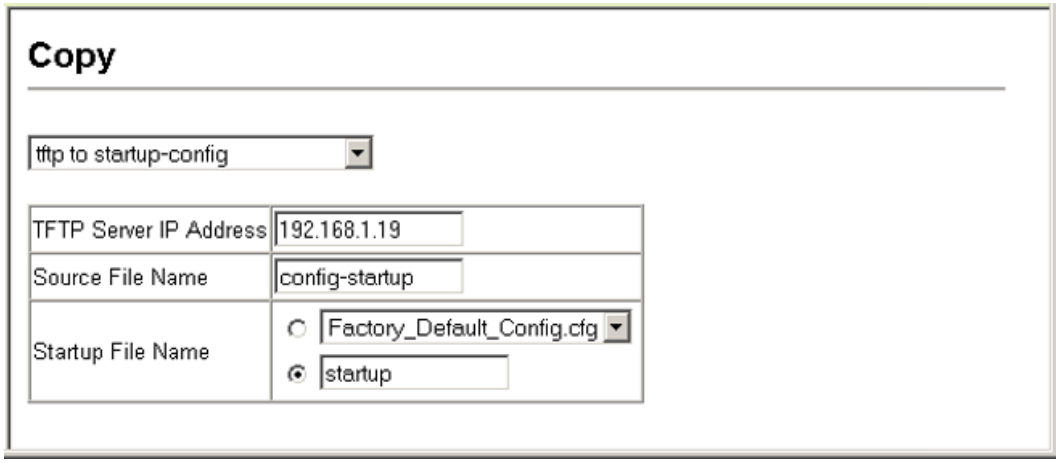


Figure 4-11 Downloading Configuration Settings for Start-Up

Downloaded from www.Manualslib.com manuals search engine

If you download to a new file name using "tftp to startup-config" or "tftp to file," the file is automatically set as the start-up configuration file. To use the new settings, reboot the system via the System/Reset menu. You can also select any configuration file as the start-up configuration by using the System/File Management/Set Start-Up page.

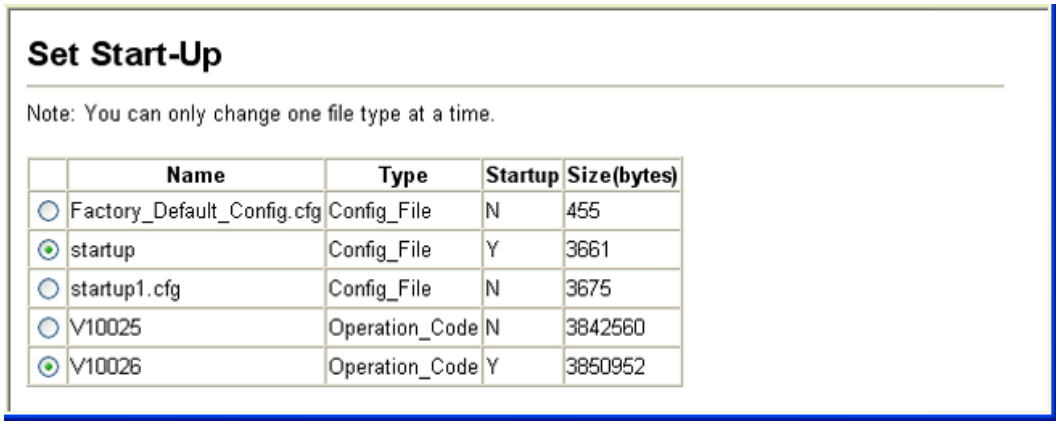


Figure 4-12 Setting the Startup Configuration Settings

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                    20-17
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

To select another configuration file as the start-up configuration, use the **boot system** command and then restart the switch.

```
Console#config
Console(config)#boot system config: startup                         20-25
Console(config)#exit
Console#reload                                                      19-5
```


Downloaded from www.Manualslib.com manuals search engine

Console Port Settings

You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial console port. Management access through the console port is controlled by various parameters, including a password, timeouts, and basic communication settings. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 0)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 0 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535; Default: 0)
- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)
- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the

Downloaded from www.Manualslib.com manuals search engine

device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud, Auto; Default: Auto)

- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)
- **Password**[2] – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login**[2] – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Console. Specify the console port connection parameters as required, then click Apply.

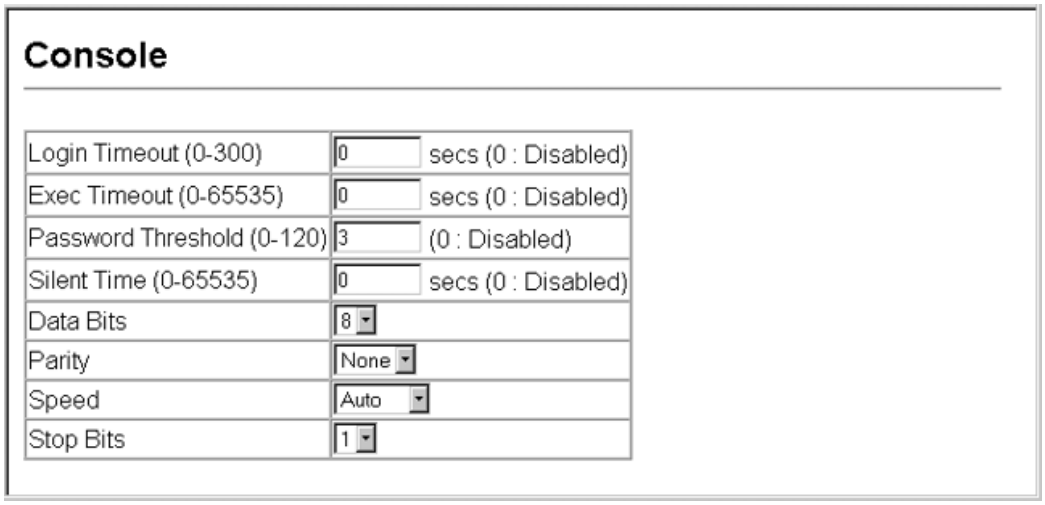


Figure 4-13 Configuring the Console Port

2. CLI only.

Downloaded from www.Manualslib.com manuals search engine

CLI – Enter Line Configuration mode for the console, then specify the connection parameters as required. To display the current console port settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line console                                    20-27
Console(config-line)#login local                                20-28
Console(config-line)#password 0 secret                          20-29
Console(config-line)#timeout login response 0                   20-30
Console(config-line)#exec-timeout 0                             20-31
Console(config-line)#password-thresh 5                          20-32
Console(config-line)#silent-time 60                             20-33
Console(config-line)#databits 8                                 20-33
Console(config-line)#parity none                                20-34
Console(config-line)#speed auto                                 20-35
Console(config-line)#stopbits 1                                 20-36
Console(config-line)#end
Console#show line console                                       20-37
 Console configuration:
  Password threshold:  5 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         60
  Baudrate:            auto
  Databits:            8
  Parity:              none
  Stopbits:            1
Console#
```

Telnet Settings

You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other various parameters set, including the TCP port number, timeouts, and a password. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **Telnet Port Number** – Sets the TCP port number for Telnet on the switch. (Default: 23)

Downloaded from www.Manualslib.com manuals search engine

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 300 seconds)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Password**[3] – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login**[3] – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

3. CLI only.

Downloaded from www.Manualslib.com manuals search engine

Web – Click System, Line, Telnet. Specify the connection parameters for Telnet access, then click Apply.

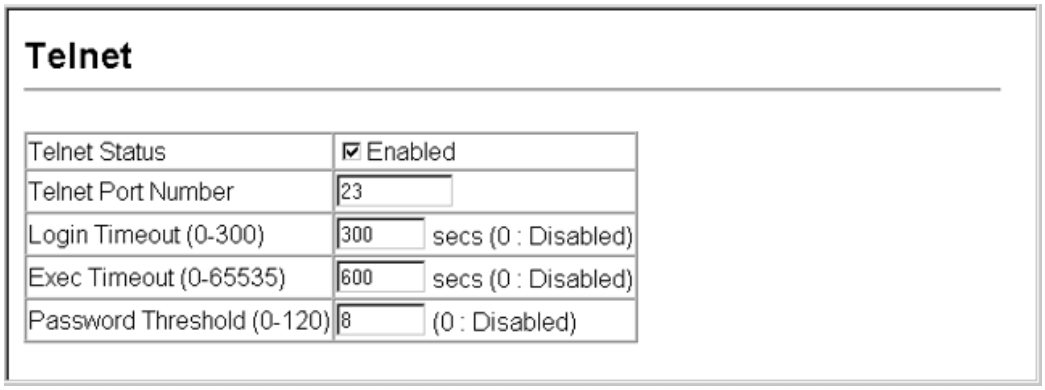


Figure 4-14 Configuring the Telnet Interface

CLI – Enter Line Configuration mode for a virtual terminal, then specify the connection parameters as required. To display the current virtual terminal settings, use the **show line** command from the Normal Exec level.

```
Console(config)#ip telnet server                                  22-20
Console(config)#ip telnet port 123                                22-20
Console(config)#line vty                                          20-27
Console(config-line)#login local                                  20-28
Console(config-line)#password 0 secret                            20-29
Console(config-line)#timeout login response 300                   20-30
Console(config-line)#exec-timeout 600                             20-31
Console(config-line)#password-thresh 3                            20-32
Console(config-line)#end
Console#show line vty                                             20-37
 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:       300 sec
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Event Logging

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

System Log Configuration

The system allows you to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 4-1 Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start

Downloaded from www.Manualslib.com manuals search engine

Table 4-1 Logging Levels (Continued)

Level	Severity Name	Description
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, Logs, System Logs. Specify System Log Status, set the level of event messages to be logged to RAM and flash memory, then click Apply.

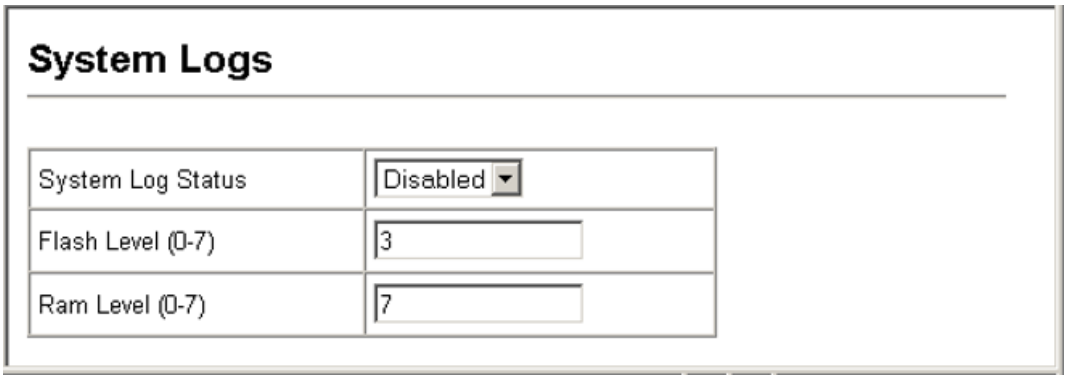


Figure 4-15 System Logs

Downloaded from www.Manualslib.com manuals search engine

CLI – Enable system logging and then specify the level of messages to be logged to RAM and flash memory. Use the **show logging** command to display the current settings.

```
Console(config)#logging on                                    20-39
Console(config)#logging history ram 0                         20-40
Console(config)#
Console#show logging ram                                      20-45
Syslog logging:           Disabled
History logging in RAM: level emergencies
Console#
```

Remote Log Configuration

The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages at or above a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

  The attribute specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Host IP List** – Displays the list of remote server IP addresses that will receive syslog messages. The maximum number of host IP addresses allowed is five.

Downloaded from www.Manualslib.com manuals search engine

- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

Web – Click System, Logs, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add. To delete an IP address, click the entry in the Host IP List, and then click Remove.

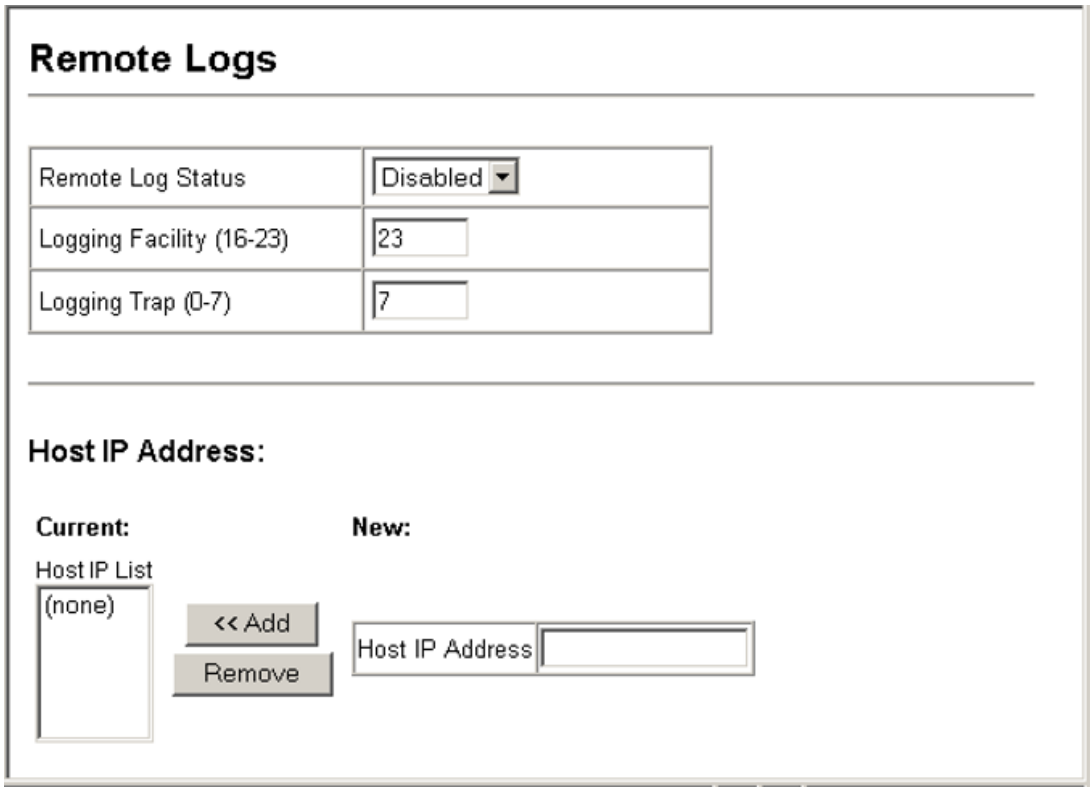


Figure 4-16 Remote Logs

Downloaded from www.Manualslib.com manuals search engine

CLI – Enter the syslog server host IP address, choose the facility type and set the logging trap.

```
Console(config)#logging host 10.1.0.9                              20-41
Console(config)#logging facility 23                                20-42
Console(config)#logging trap 4                                     20-43
Console(config)#logging trap
Console(config)#exit
Console#show logging trap                                          20-45
Syslog logging:               Enabled
REMOTELOG status:             Disabled
REMOTELOG facility type:      local use 7
REMOTELOG level type:         Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Displaying Log Messages

Use the Logs page to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Log, Logs.

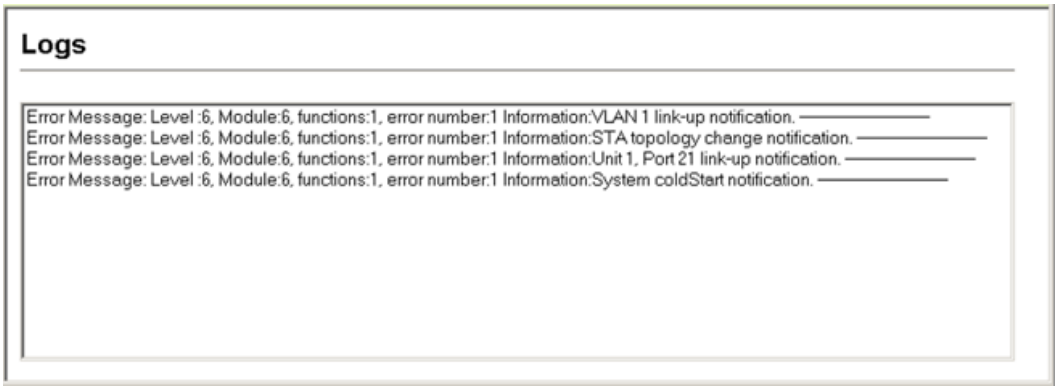

Logs
Error Message: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:STA topology change notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 21 link-up notification.
Error Message: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification.

Figure 4-17 Displaying Logs

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows the event message stored in RAM.

```
Console#show log ram                                              20-45
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

Sending Simple Mail Transfer Protocol Alerts

To alert system administrators of problems, the switch can use SMTP (Simple Mail Transfer Protocol) to send email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

Command Attributes

- **Admin Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Email Source Address** – Sets the email address used for the "From" field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.
- **Severity** – Sets the syslog severity threshold level (see table on page 4-29) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- **SMTP Server List** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails. Use the New SMTP Server text field and the Add/Remove buttons to configure the list.
- **Email Destination Address List** – Specifies the email recipients of alert messages. You can specify up to five recipients. Use the New Email Destination Address text field and the Add/Remove buttons to configure the list.

Downloaded from www.Manualslib.com manuals search engine

Web – Click System, Log, SMTP. Enable SMTP, specify a source email address, and select the minimum severity level. To add an IP address to the SMTP Server List, type the new IP address in the SMTP Server field and click Add. To delete an IP address, click the entry in the SMTP Server List and click Remove. Specify up to five email addresses to receive the alert messages, and click Apply.

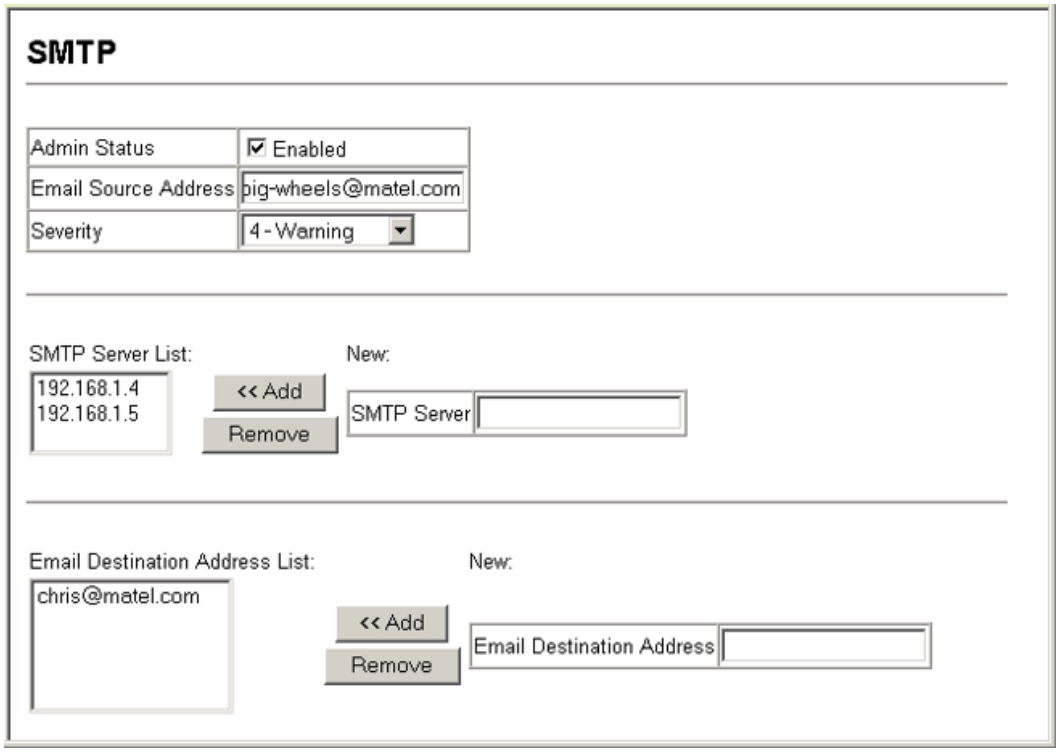


Figure 4-18 Enabling and Configuring SMTP Alerts

Downloaded from www.Manualslib.com manuals search engine

CLI – Enter the IP address of at least one SMTP server, set the syslog severity level to trigger an email message, and specify the switch (source) and up to five recipient (destination) email addresses. Enable SMTP with the **logging sendmail** command to complete the configuration. Use the **show logging sendmail** command to display the current SMTP configuration.

```
Console(config)#logging sendmail host 192.168.1.4                20-48
Console(config)#logging sendmail level 3                         20-49
Console(config)#logging sendmail source-email
   big-wheels@matel.com                                          20-50
Console(config)#logging sendmail destination-email
   chris@matel.com                                               20-50
Console(config)#logging sendmail                                 20-51
Console(config)#exit
Console#show logging sendmail                                    20-52
SMTP servers
-----------------------------------------------
  1. 192.168.1.4

SMTP Minimum Severity Level: 4

SMTP destination email addresses
-----------------------------------------------
  1. chris@matel.com

SMTP Source Email Address: big-wheels@matel.com

SMTP Status:                Enabled
Console#
```

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch. When prompted, confirm that you want reset the switch.

Figure 4-19 Resetting the System

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the reload command to restart the switch.

```
Console#reload                                                    19-5
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See "calendar set" on page 20-58.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Configuring SNTP

You can configure the switch to send time synchronization requests to time servers.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP client. This requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

Downloaded from www.Manualslib.com manuals search engine

- **SNTP Server** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.

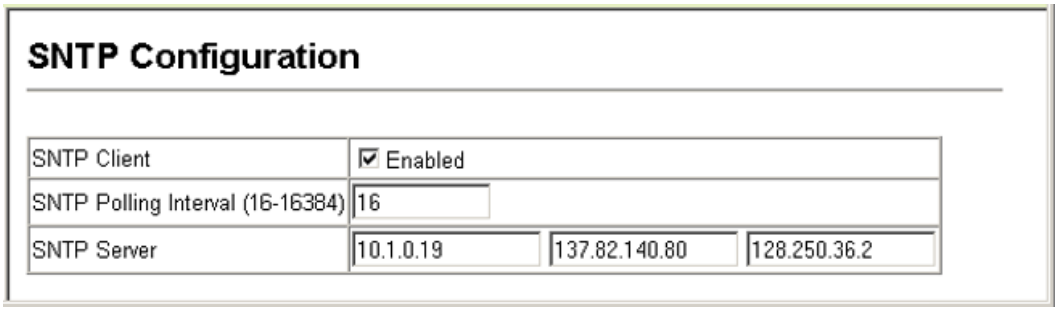


Figure 4-20 SNTP Configuration

CLI – This example configures the switch to operate as an SNTP client and then displays the current time and settings.

```
Console(config)#sntp client                                          20-53
Console(config)#sntp poll 16                                         20-55
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.220-54
Console(config)#exit
Console#show sntp                                                    20-56
Current time:  Jan  6 14:56:05 2004
Poll interval: 60
Current  mode:  unicast
SNTP status : Enabled
SNTP server 10.1.0.19 137.82.140.80 128.250.36.2
Current server: 128.250.36.2
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours (0-13)** – The number of hours before/after UTC.
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.

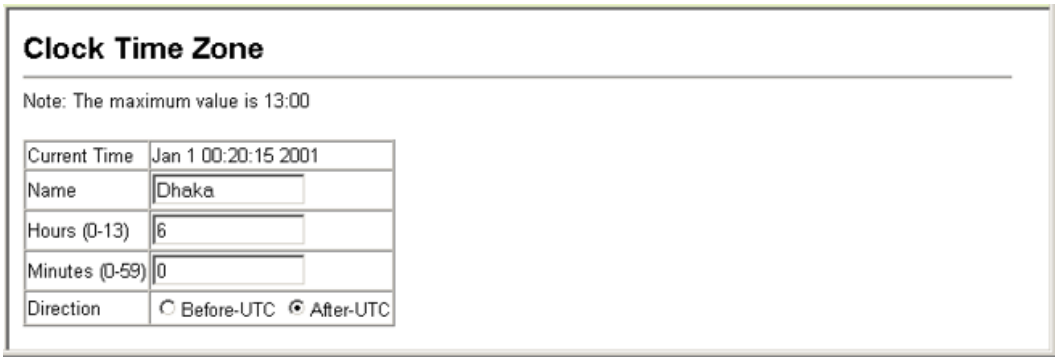


Figure 4-21 Clock Time Zone

CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC   20-57
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Chapter 5
Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Downloaded from www.Manualslib.com manuals search engine

Access to the switch using from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 5-1 SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	A user name match only

Downloaded from www.Manualslib.com manuals search engine

Table 5-1 SNMPv3 Security Models and Levels (Continued)

Model	Level	Group	Read View	Write View	Notify View	Security
v3	AuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

Note: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

Downloaded from www.Manualslib.com manuals search engine

Enabling the SNMP Agent

Enables SNMPv3 service for all management clients (i.e., versions 1, 2c, 3).

Command Attributes

SNMP Agent Status – Enables SNMP on the switch.

Web – Click SNMP, Agent Status. Enable the SNMP Agent by marking the Enabled checkbox, and click Apply.

Figure 5-1 Enabling the SNMP Agent

CLI – The following example enables SNMP on the switch.

```
Console(config)#snmp-server                                    21-2
Console(config)#
```

Setting Community Access Strings

You may configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – The switch supports up to five community strings.
- **Current** – Displays a list of the community strings currently configured.

Downloaded from www.Manualslib.com manuals search engine

- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.
  Default strings: "public" (read-only access), "private" (read/write access)
  Range: 1-32 characters, case sensitive
- **Access Mode** – Specifies the access rights for the community string:
  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.

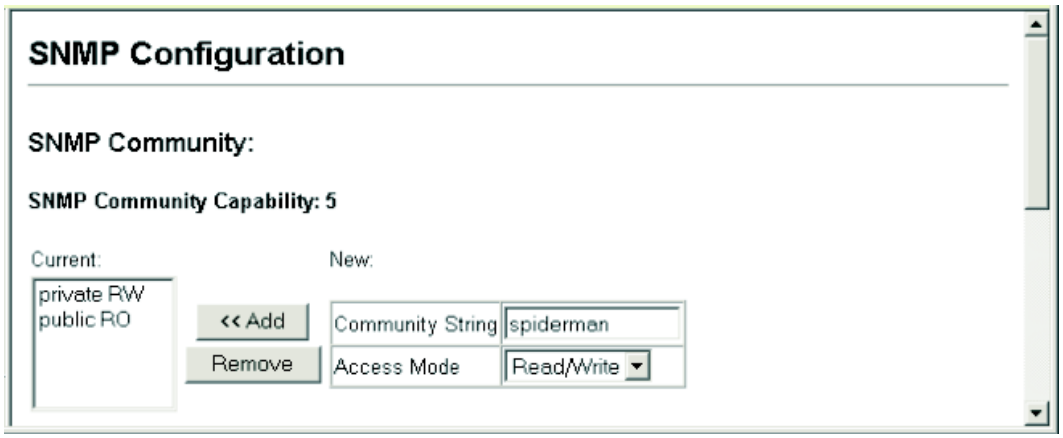


Figure 5-2 Configuring SNMP Community Strings

CLI – The following example adds the string "spiderman" with read/write access.

```
Console(config)#snmp-server community spiderman rw          21-4
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- If you specify an SNMP Version 3 host, then the "Trap Manager Community String" is interpreted as an SNMP user name. If you use V3 authentication or encryption options (authNoPriv or authPriv), the user name must first be defined in the SNMPv3 Users page (page 5-12). Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the no authentication (noAuth) option, an SNMP user account will be automatically generated, and the switch will authorize SNMP access for the host.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 5-4).
  2. Enable trap informs as described in the following pages.
  3. Create a view with the required notification messages (page 5-24).
  4. Create a group that includes the required notify view (page 5-18).

Downloaded from www.Manualslib.com manuals search engine

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 5-4).
2. Enable trap informs as described in the following pages.
3. Create a view with the required notification messages (page 5-24).
4. Create a group that includes the required notify view (page 5-18).
5. Specify a remote engine ID where the user resides (page 5-11).
6. Then configure a remote user (page 5-15).

Command Attributes

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Current** – Displays a list of the trap managers currently configured.
- **Trap Manager IP Address** – IP address of a new management station to receive notification messages.
- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. Though you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Configuration page (for Version 1 or 2c clients), or define a corresponding "User Name" in the SNMPv3 Users page (for Version 3 clients). (Range: 1-32 characters, case sensitive)
- **Trap UDP Port** – Specifies the UDP port number used by the trap manager.
- **Trap Version** – Indicates if the user is running SNMP v1, v2c, or v3. (Default: v1)
- **Trap Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

Downloaded from www.Manualslib.com manuals search engine

- **Trap Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
  - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Enable Authentication Traps**[4] – Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)
- **Enable Link-up and Link-down Traps**[4] – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

4. These are legacy notifications and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 5-18).

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, Configuration. Enter the IP address and community string for each management station that will receive trap messages, specify the UDP port, SNMP trap version, trap security level (for v3 clients), trap inform settings (for v2c/v3 clients), and then click Add. Select the trap types required using the check boxes for Authentication and Link-up/down traps, and then click Apply.

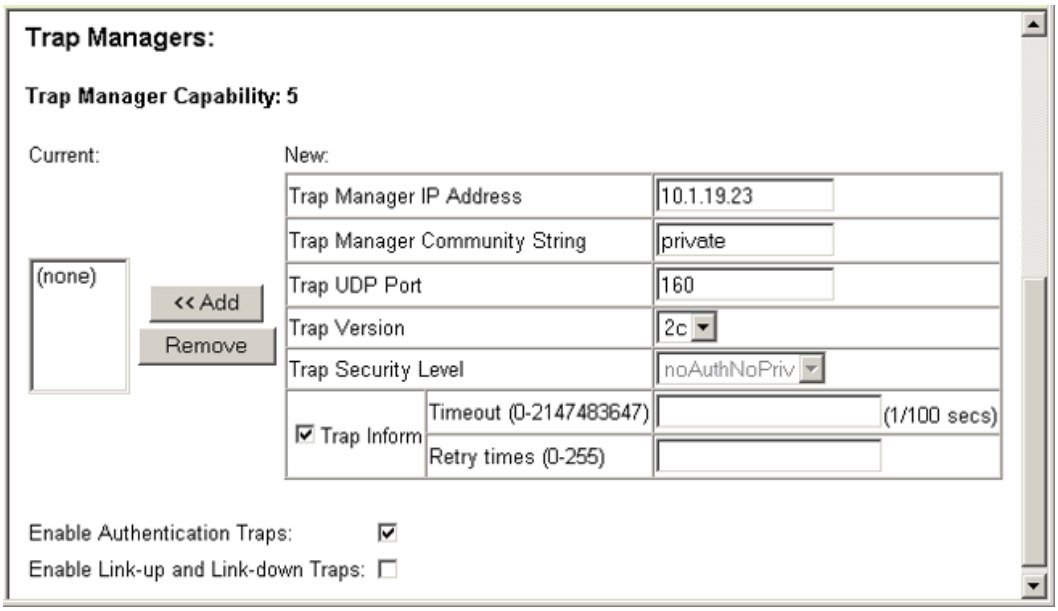


Figure 5-3 Configuring SNMP Trap Managers

CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 private version 2c
 udp-port 162                                                  21-6
Console(config)#snmp-server enable traps authentication       21-9
```


Downloaded from www.Manualslib.com manuals search engine

Configuring SNMPv3 Management Access

To configure SNMPv3 management access to the switch, follow these steps:

1. If you want to change the default engine ID, do so before configuring other SNMP parameters.
2. Specify read and write access views for the switch MIB tree.
3. Configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).
4. Assign SNMP users to groups, along with their specific authentication and privacy passwords.

Setting a Local Engine ID

An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

A new engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, SNMPv3, Engine ID. Enter an ID of up to 26 hexadecimal characters and then click Save.

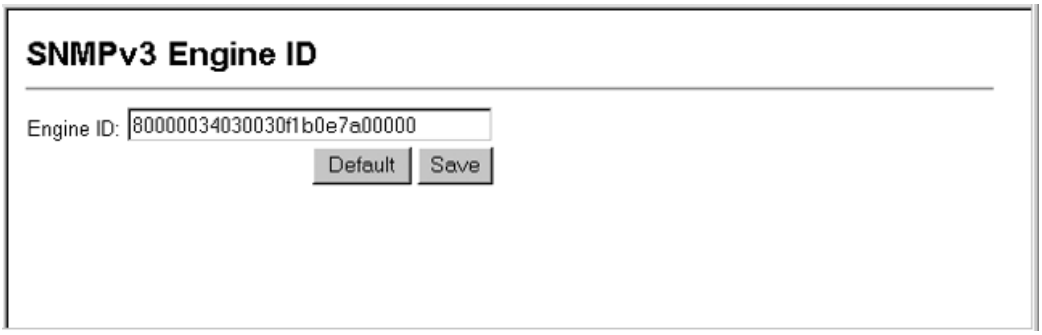


Figure 5-4 Setting the SNMPv3 Engine ID

CLI – This example sets an SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id local 12345abcdef       21-10
Console(config)#exit
Console#show snmp engine-id                                   21-12
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1
Console#
```

Specifying a Remote Engine ID

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Specifying Trap Managers and Trap Types" on page 5-6 and "Configuring Remote SNMPv3 Users" on page 5-15.)

The engine ID can be specified by entering 10 to 64 hexadecimal characters. If less than 64 characters are specified, trailing zeroes are added to the value. For example, the value "0123456789" is equivalent to "0123456789" followed by 60 zeroes.

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, SNMPv3, Remote Engine ID. Enter an ID of up to 26 hexadecimal characters and then click Save.

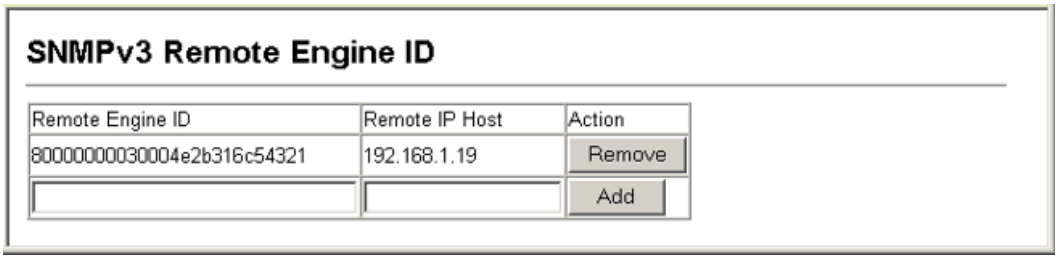


Figure 5-5 Setting an Engine ID

CLI – This example specifies a remote SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id remote 54321 192.168.1.19      21-10
Console(config)#exit
Console#show snmp engine-id                                          21-12
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                          IP address
80000000030004e2b316c54321                                    192.168.1.19
Console#
```

Configuring SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, or notify view.

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).

Downloaded from www.Manualslib.com manuals search engine

  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.
- **Actions** – Enables the user to be assigned to another SNMPv3 group.

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, SNMPv3, Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.

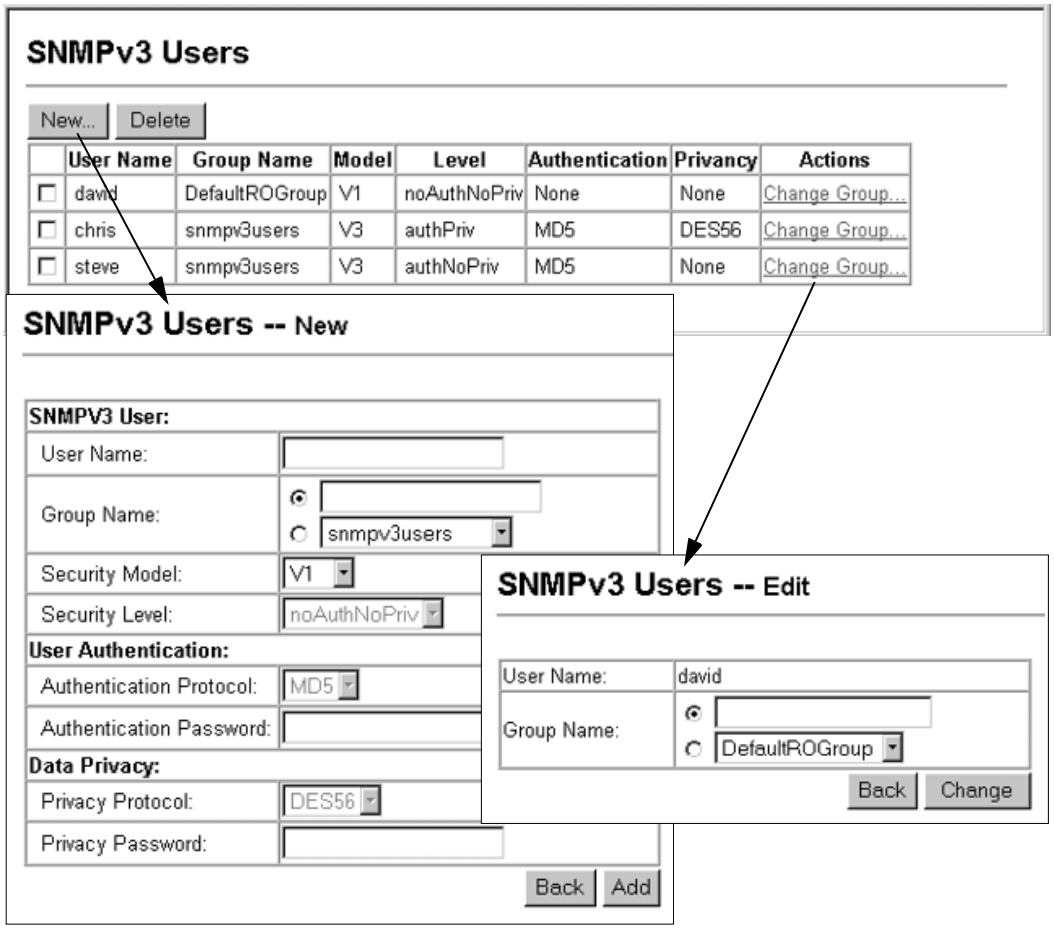


Figure 5-6 Configuring SNMPv3 Users

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user chris group r&d v3 auth md5
 greenpeace priv des56 einstien                                    21-18
Console(config)#exit
Console#show snmp user                                             21-20
EngineId: 800000340300001f488f5200000
User Name: chris
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring Remote SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read and a write view.

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. (See "Specifying Trap Managers and Trap Types" on page 5-6 and "Specifying a Remote Engine ID" on page 5-11.)

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Engine ID** – The engine identifier for the SNMP agent on the remote device where the remote user resides. Note that the remote engine identifier must be specified before you configure a remote user. (See "Specifying a Remote Engine ID" on page 5-11.)
- **Remote IP** – The Internet address of the remote device where the user resides.

Downloaded from www.Manualslib.com manuals search engine

- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v1)
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, SNMPv3, Remote Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete.

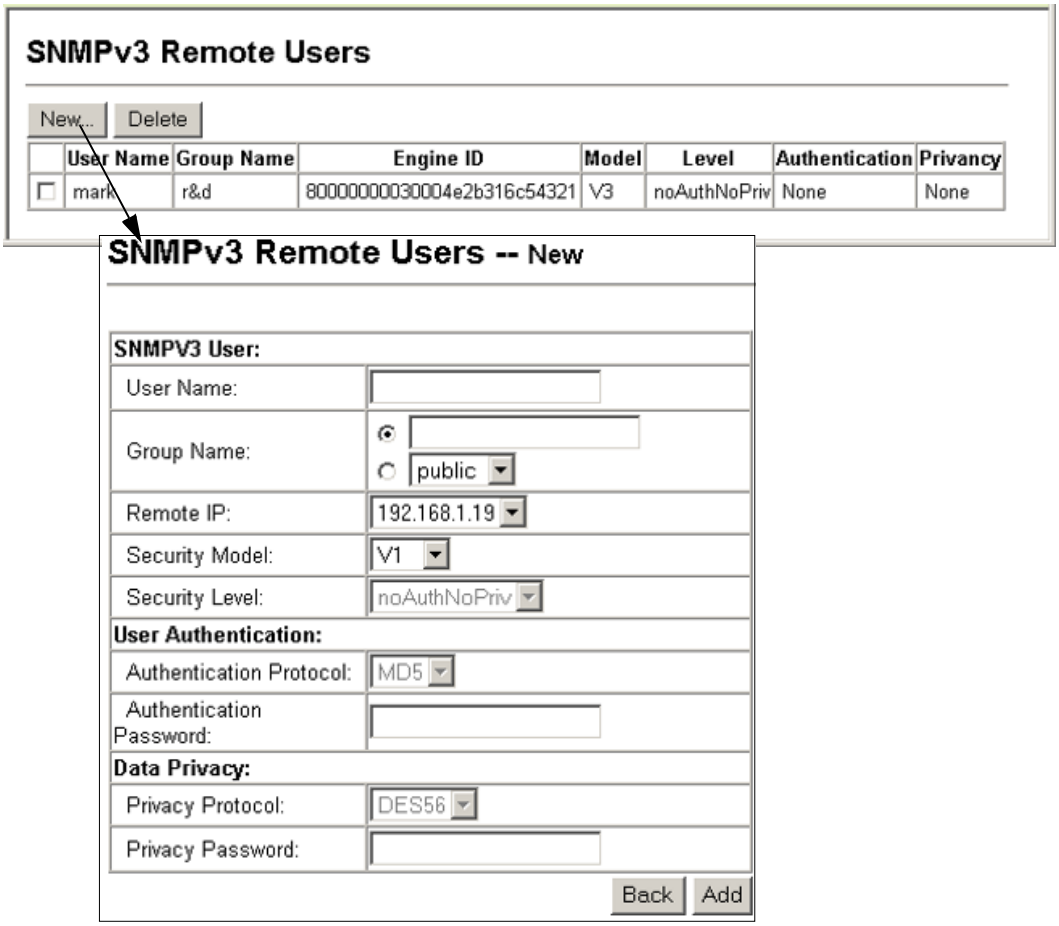


Figure 5-7 Configuring Remote SNMPv3 Users

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user mark group r&d remote 192.168.1.19
 v3 auth md5 greenpeace priv des56 einstien                    21-18
Console(config)#exit
Console#show snmp user                                         21-20
No user exist.

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring SNMPv3 Groups

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

Command Attributes

- **Group Name** – The name of the SNMP group. (Range: 1-32 characters)
- **Model** – The group security model; SNMP v1, v2c or v3.
- **Level** – The security level used for the group:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications.
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Read View** – The configured view for read access. (Range: 1-64 characters)
- **Write View** – The configured view for write access. (Range: 1-64 characters)

Downloaded from www.Manualslib.com manuals search engine

- **Notify View** – The configured view for notifications. (Range: 1-64 characters)

Table 5-2 Supported Notification Messages

Object Label	Object ID	Description
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.

Downloaded from www.Manualslib.com manuals search engine

Table 5-2 Supported Notification Messages (Continued)

Object Label	Object ID	Description
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

Downloaded from www.Manualslib.com manuals search engine

Table 5-2 Supported Notification Messages (Continued)

Object Label	Object ID	Description
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.
Private Traps -		
swPowerStatus ChangeTrap	1.3.6.1.4.1.202.40.2.6.2.1.0.1	This trap is sent when the power state changes.
swFanFailureTrap	1.3.6.1.4.1.202.40.2.6.2.1.0.17	This trap is sent when the fan fails.
swFanRecoverTrap	1.3.6.1.4.1.202.40.2.6.2.1.0.18	This trap is sent when the fan failure has recovered.
swIpFilterRejectTrap	1.3.6.1.4.1.202.40.2.6.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swSmtpConnFailure Trap	1.3.6.1.4.1.202.40.2.6.2.1.0.41	This trap is triggered if the SMTP system cannot open a connection to the mail server successfully.
swMainBoardVer MismatchNotificaiton	1.3.6.1.4.1.202.40.2.6.2.1.0.56	This trap is sent when the slave board version is mismatched with the master board version. This trap binds two objects, the first object indicates the master version, whereas the second represents the slave version.
swModuleVer MismatchNotificaiton	1.3.6.1.4.1.202.40.2.6.2.1.0.57	This trap is sent when the slide-in module version is mismatched with the main board version.

Downloaded from www.Manualslib.com manuals search engine

Table 5-2 Supported Notification Messages (Continued)

Object Label	Object ID	Description
swThermalRising Notification	1.3.6.1.4.1.202.40.2.6.2.1.0.58	This trap is sent when the temperature exceeds the switchThermalActionRisingThreshold.
swThermalFalling Notification	1.3.6.1.4.1.202.40.2.6.2.1.0.59	This trap is sent when the temperature falls below the switchThermalActionFallingThreshold.
swModuleInsertion Notificaiton	1.3.6.1.4.1.202.40.2.6.2.1.0.60	This trap is sent when a module is inserted.
swModuleRemoval Notificaiton	1.3.6.1.4.1.202.40.2.6.2.1.0.61	This trap is sent when a module is removed.

* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu (page 5-9).

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, SNMPv3, Groups. Click New to configure a new group. In the New Group page, define a name, assign a security model and level, and then select read, write, and notify views. Click Add to save the new group and return to the Groups list. To delete a group, check the box next to the group name, then click Delete.

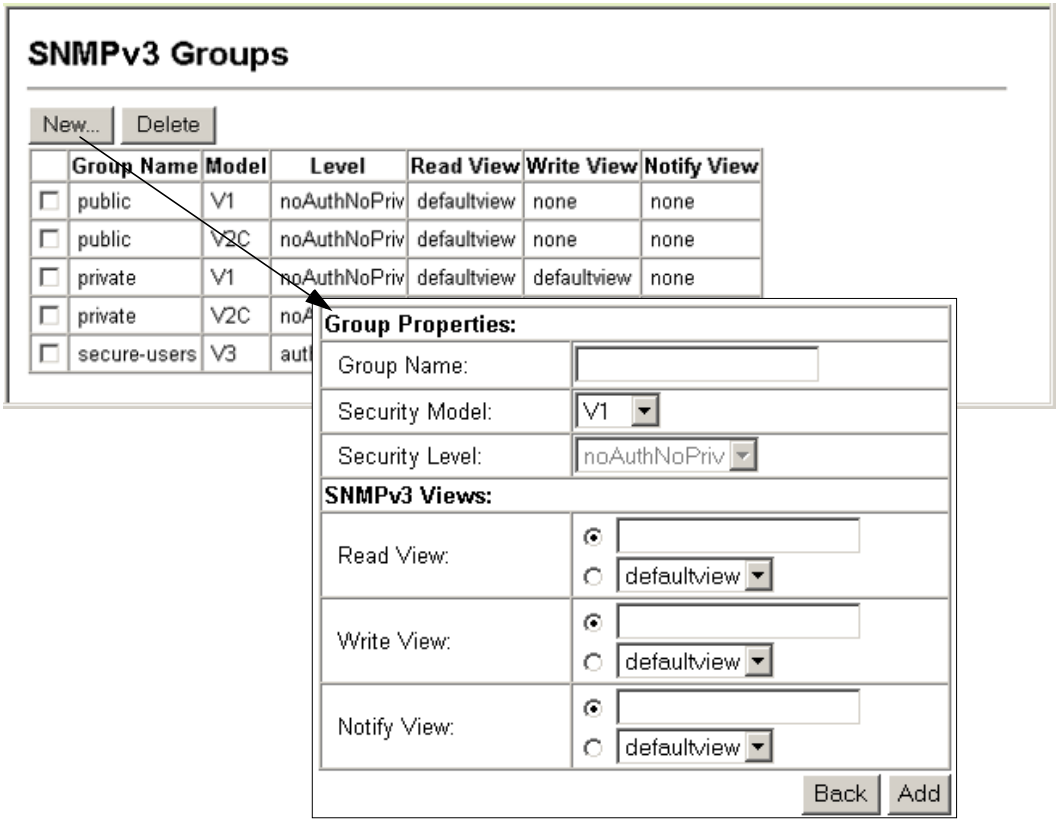


Figure 5-8 Configuring SNMPv3 Groups

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the **snmp-server group** command to configure a new group, specifying the security model and level, and restricting MIB access to defined read and write views.

```
Console(config)#snmp-server group secure-users v3 priv read
 defaultview write defaultview notify defaultview            21-15
Console(config)#exit
Console#show snmp group                                      21-16
:
Group Name: secure-users
Security Model: v3
Read View: defaultview
Write View: defaultview
Notify View: defaultview
Storage Type: nonvolatile
Row Status: active

Console#
```

Setting SNMPv3 Views

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

Command Attributes

- **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- **View OID Subtrees** – Shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view.
- **Edit OID Subtrees** – Allows you to configure the object identifiers of branches within the MIB tree. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Downloaded from www.Manualslib.com manuals search engine

Web – Click SNMP, SNMPv3, Views. Click New to configure a new view. In the New View page, define a name and specify OID subtrees in the switch MIB to be included or excluded in the view. Click Back to save the new view and return to the SNMPv3 Views list. For a specific view, click on View OID Subtrees to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings. To delete a view, check the box next to the view name, then click Delete.

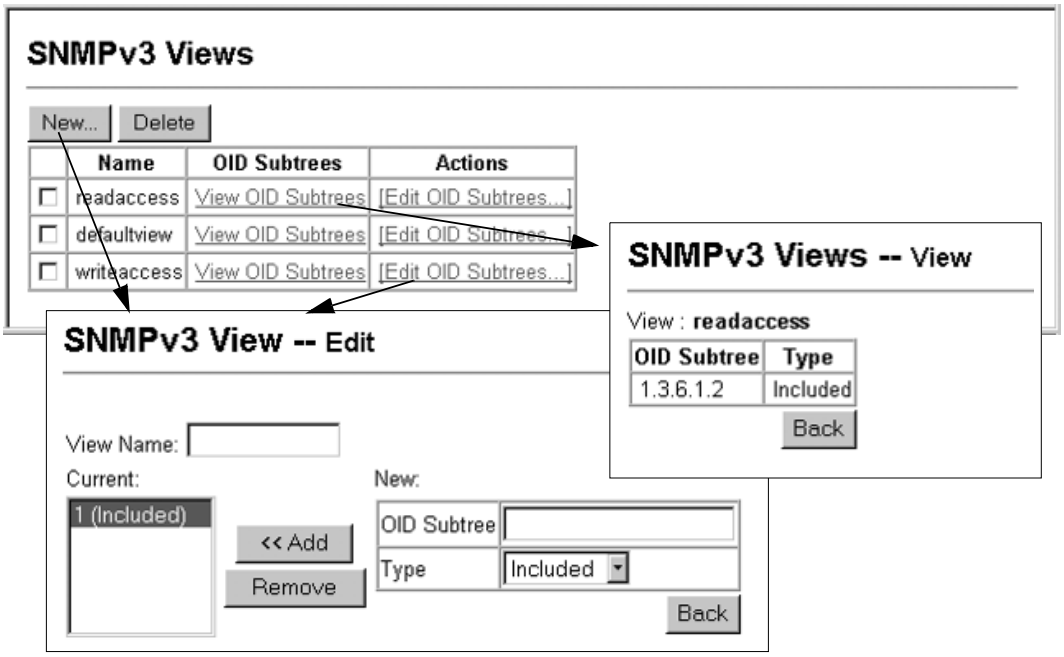


Figure 5-9 Configuring SNMPv3 Views

Downloaded from www.Manualslib.com manuals search engine

CLI – Use the **snmp-server view** command to configure a new view. This example view includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
  included                                                    21-13
Console(config)#exit
Console#show snmp view                                        21-14
View Name: ifEntry.a
Subtree OID: 1.3.6.1.2.1.2.2.1.1.*
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: readaccess
Subtree OID: 1.3.6.1.2
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 6
USER AUTHENTICATION

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access[5] to the data ports. This switch provides secure network management access using the following options:

- User Accounts – Manually configure management access rights for users.
- Authentication Settings – Use remote authentication to configure access rights.
- HTTPS Settings – Provide a secure web connection.
- SSH Settings – Provide a secure shell (for secure Telnet access).
- Port Security – Configure secure addresses for individual ports.
- 802.1X – Use IEEE 802.1X port authentication to control access to specific ports.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.

Configuring User Accounts

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

5. For other methods of controlling client access, see "Client Security" on page 7-1.

Downloaded from www.Manualslib.com manuals search engine

The default guest name is "guest" with the password "guest." The default administrator name is "admin" with the password "admin."

Command Attributes

- **Account List** – Displays the current list of user accounts and associated access levels. (Defaults: admin, and guest)
- **New Account** – Displays configuration settings for a new account.
  - **User Name** – The name of the user.
    (Maximum length: 8 characters; maximum number of users: 16)
  - **Access Level** – Specifies the user level.
    (Options: Normal and Privileged)
  - **Password** – Specifies the user password.
    (Range: 0-8 characters plain text, case sensitive)
- **Change Password** – Sets a new password for the specified user.

Web – Click Security, User Accounts. To configure a new user account, enter the user name, access level, and password, then click Add. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again, then click Apply.

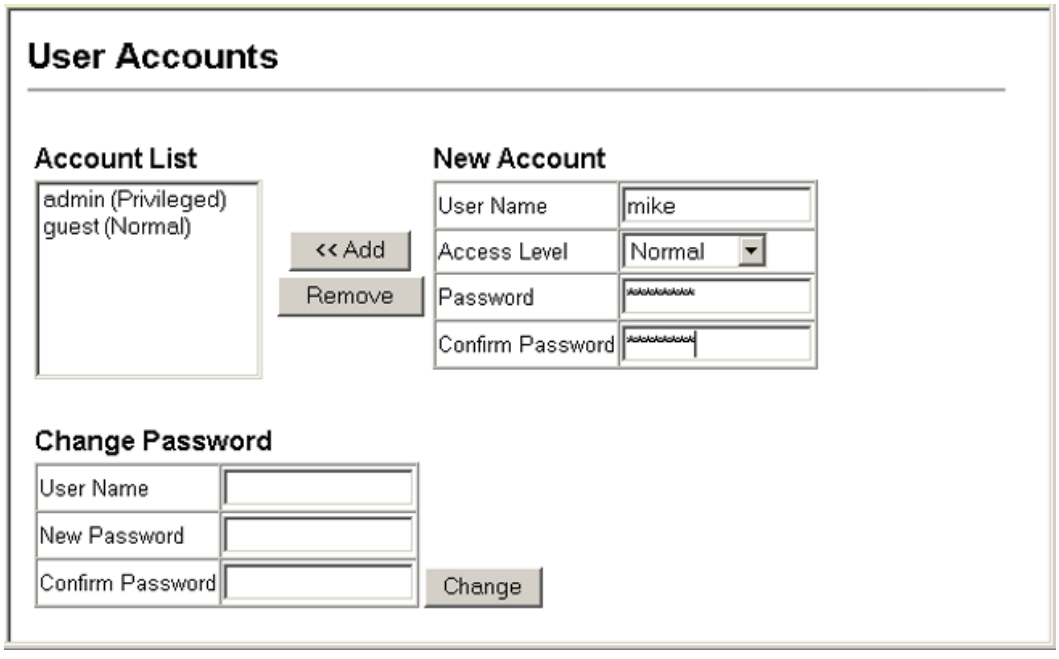


Figure 6-1 User Accounts

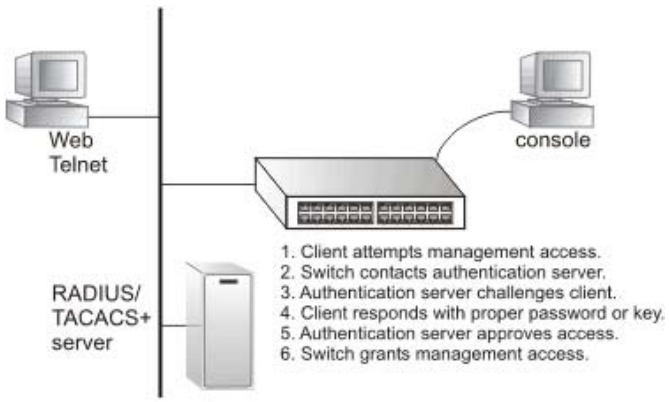
Downloaded from www.Manualslib.com manuals search engine

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                    22-2
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.



Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS- aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5).
- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **Radius** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.
- **RADIUS Settings**
  - **Global** – Provides globally applicable RADIUS settings.

Downloaded from www.Manualslib.com manuals search engine

- **ServerIndex** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
- **Server IP Address** – Address of authentication server. (Default: 10.1.0.1)
- **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

• **TACACS Settings**

- **Server IP Address** – Address of the TACACS+ server. (Default: 10.11.12.13)
- **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See "username" on page 22-2.)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.

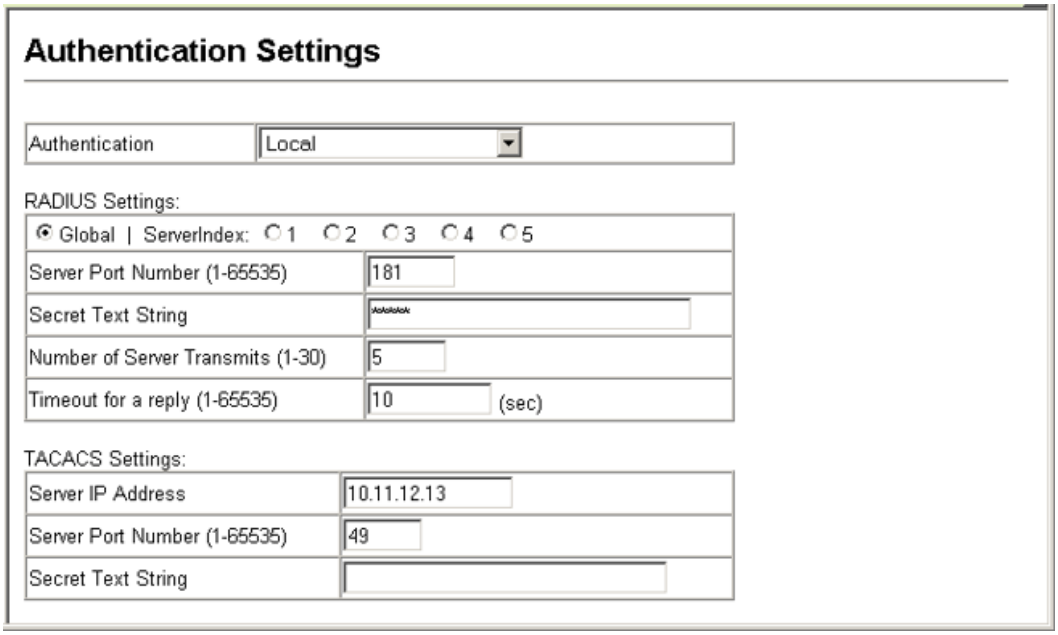


Figure 6-2 Authentication Server Settings

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                    22-5
Console(config)#radius-server port 181                         22-10
Console(config)#radius-server key green                        22-10
Console(config)#radius-server retransmit 5                     22-11
Console(config)#radius-server timeout 10                       22-11
Console(config)#radius-server 1 host 192.168.1.25              22-13
Console(config)#exit
Console#show radius-server                                     22-12

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   181
 Retransmit times:                     5
 Request timeout:                      10
```


Downloaded from www.Manualslib.com manuals search engine

```
Server 1:
 Server IP address: 192.168.1.25
 Communication key with RADIUS server: *****
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10

Console#config
Console(config)#authentication login tacacs                    22-5
Console(config)#tacacs-server host 10.20.30.40                 22-13
Console(config)#tacacs-server port 200                         22-14
Console(config)#tacacs-server key green                        22-14
Console(config)#exit
Console#show tacacs-server                                     22-15
Server IP address:                      10.20.30.40
 Communication key with tacacs server: *****
 Server port number:                    200
Console(config)#
```

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
  A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 6.2 or above.

Downloaded from www.Manualslib.com manuals search engine

- The following web browsers and operating systems currently support HTTPS:

Table 6-1 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 6-9.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. (Default: Port 443)

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.

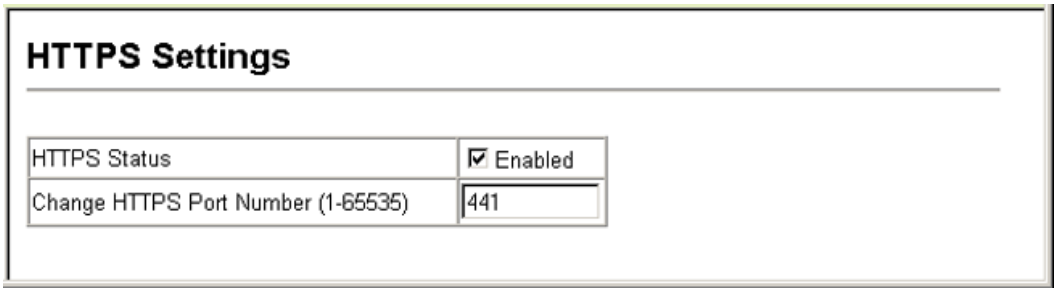


Figure 6-3 HTTPS Settings

CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server                    22-17
Console(config)#ip http secure-port 441                  22-18
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Note: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate                                    20-17
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type "reload" at the command prompt:

```
Console#reload
```


Downloaded from www.Manualslib.com manuals search engine

Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Command Usage

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the **Authentication Settings** page (page 6-3). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

Downloaded from www.Manualslib.com manuals search engine

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956 10825913212890233
   76546801726272571413428762941301196195566782 59566410486957427888146206
   51941746772984865468615717739390164779355942303577413098022737087794545240839
   71752646358058176716709574804776117

3. *Import Client's Public Key to the Switch* – Use the **copy tftp public-key** command (page 20-17) to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 6-1.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

   1024 35 134108168560989392104094492015542534763164192187295892114317388 0
   05553616163105177594083868631109291232226828519254374603100937187721199696317
   81366277414168985132049117204830339254324101637997592371449011938006090253948
   40848271781943722884025331159521348610229029789827213532671316294325328189150
   45306393916643 steve@192.168.1.19

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

Downloaded from www.Manualslib.com manuals search engine

6. *Authentication* – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.
b. The switch compares the client's public key to those stored in memory.
c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.
d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Downloaded from www.Manualslib.com manuals search engine

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
c. The client sends a signature generated using the private key to the switch.
d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the preceding section (Command Usage).

Field Attributes

- **Public-Key of Host-Key** – The public key for the host.
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA: The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.

Downloaded from www.Manualslib.com manuals search engine

- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA, DSA, Both: Default: Both)
  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

  Note: The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory to flash memory). Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.
- **Generate** – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.
- **Clear** – This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, SSH, Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click Generate.

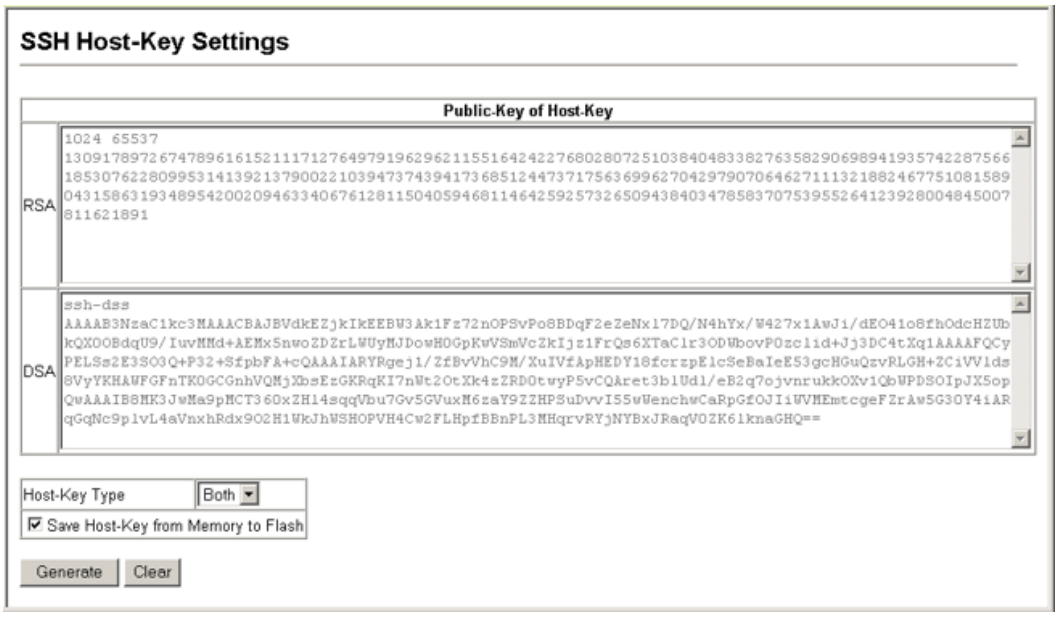


Figure 6-4 SSH Host-Key Settings

Downloaded from www.Manualslib.com manuals search engine

CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate                              22-28
Console#ip ssh save host-key                                         22-30
Console#show public-key host                                         22-32
Host:
RSA:
1024 65537
12725092254492640213133651454613118967905519236007602865300676l
82409690947448320102524878965977592168322225584652387791546479807 39
63140338692579310510576521224305280786588548578927260293786608923 68
41423275912127603259196836970534393364384452233351882871738968945 11
72929051081391964202519093210432857904576489l
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlas
fEthIwmj hLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6v
jO9XTs7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6
DkZAAAAFQCNZn/x17dwpW8RrVDQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1
TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeF
Y5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG Nq375R55yRxFvmcGIn/Q7Iph
PqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOIRTMFy3iUXtvGyQAOV
Sy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAgPNWKV6W
0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

Configuring the SSH Server

The SSH server includes basic settings for authentication.

Field Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt.
  (Range: 1 to 120 seconds; Default: 120 seconds)

Downloaded from www.Manualslib.com manuals search engine

- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- **SSH Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default: 768)
  - The server key is a private key that is never shared outside the switch.
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.

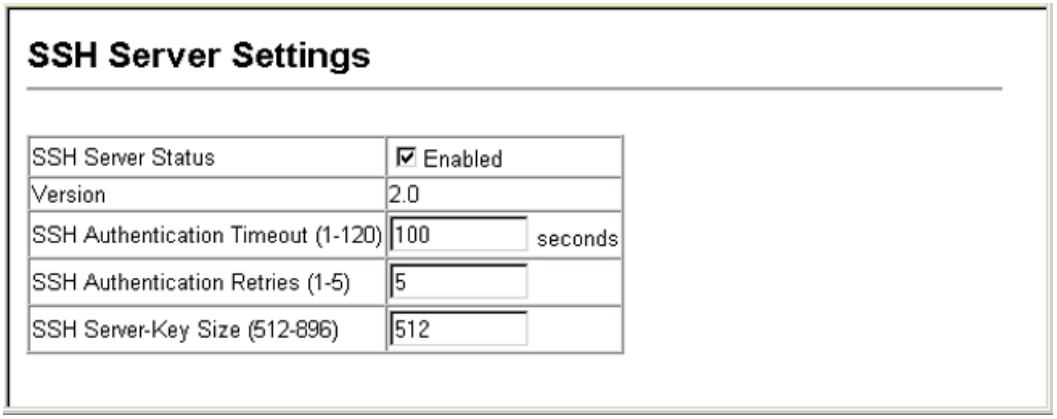


Figure 6-5 SSH Server Settings

Downloaded from www.Manualslib.com manuals search engine

CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disables this connection.

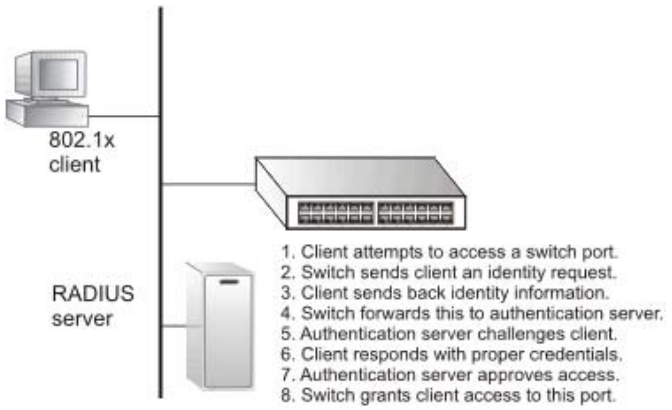
```
Console(config)#ip ssh server                                    22-25
Console(config)#ip ssh timeout 100                               22-26
Console(config)#ip ssh authentication-retries 5                  22-27
Console(config)#ip ssh server-key size 512                       22-27
Console(config)#end
Console#show ip ssh                                              22-31
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh                                                 22-31
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   2.0      cipher-3des   session-started
Console#disconnect 0                                             20-36
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring 802.1X Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.


802.1x
client
RADIUS
server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5). TLS, TTLS, and PEAP will be supported in future

Downloaded from www.Manualslib.com manuals search engine

releases. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- The IP address of the RADIUS server must be specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1x "Auto" mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)

Downloaded from www.Manualslib.com manuals search engine

Displaying 802.1X Global Settings

The 802.1X protocol provides port authentication.

Command Attributes

802.1X System Authentication Control – The global setting for 802.1X.

Web – Click Security, 802.1X, Information.

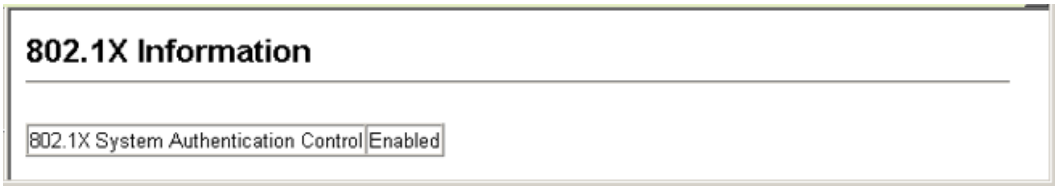


Figure 6-6 802.1X Global Information

CLI – This example shows the default global setting for 802.1X.

```
Console#show dot1x                                              22-41
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status       Operation Mode   Mode              Authorized
1/1        disabled       Single-Host      ForceAuthorized     n/a
1/2        disabled       Single-Host      ForceAuthorized     n/a
:
802.1X Port Details

802.1X is disabled on port 1/1
:
802.1X is disabled on port 26
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring 802.1X Global Settings

The 802.1X protocol provides port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

Command Attributes

802.1X System Authentication Control – Sets the global setting for 802.1X. (Default: Disabled)

Web – Select Security, 802.1X, Configuration. Enable 802.1X globally for the switch, and click Apply.

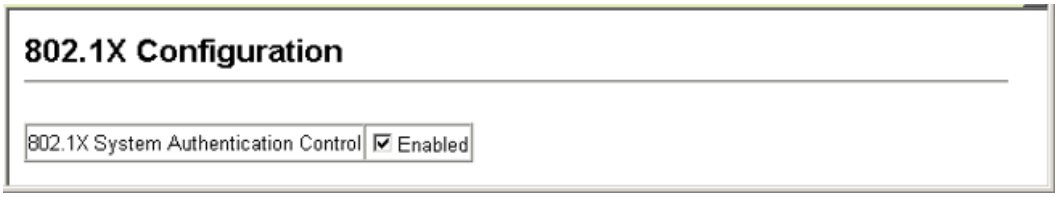


Figure 6-7 802.1X Global Configuration

CLI – This example enables 802.1X globally for the switch.

```
Console(config)#dot1x system-auth-control                    22-35
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Port Settings for 802.1X

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

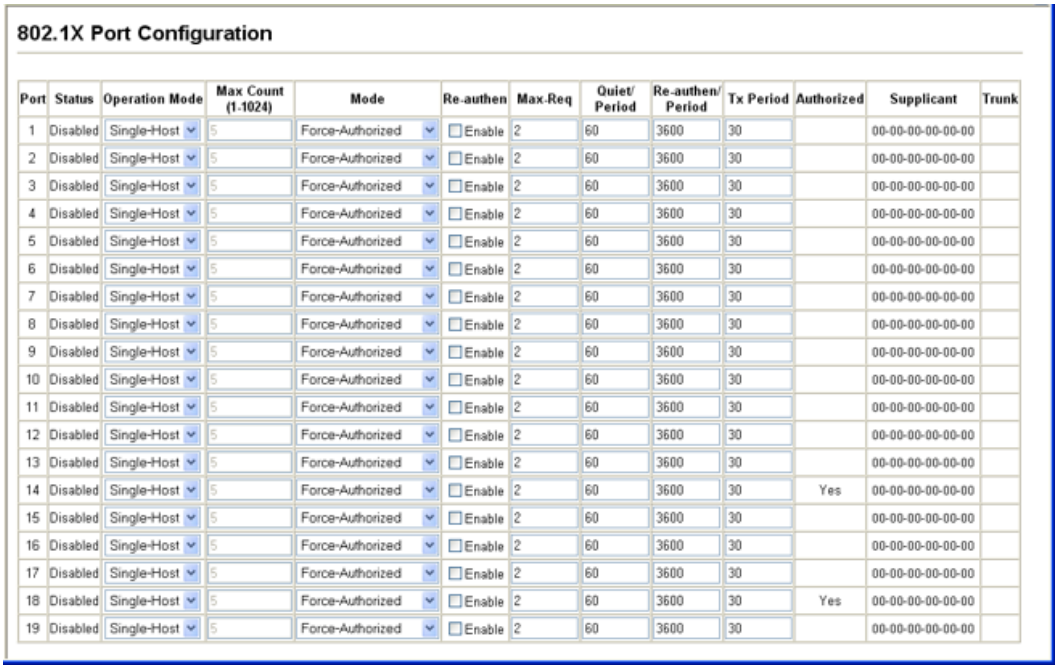
Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port. (Default: Disabled)
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host; Default: Single-Host)
- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. (Default: Disabled)
- **Max Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Quiet Period** – Sets the time that a switch port waits after the Max Request count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)

Downloaded from www.Manualslib.com manuals search engine

- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1X, Port Configuration. Modify the parameters required, and click Apply.



802.1X Port Configuration

Port	Status	Operation Mode	Max Count (1-1024)	Mode	Re-authen	Max-Req	Quiet/ Period	Re-authen/ Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
2	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
7	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
8	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
9	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
10	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
11	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
12	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
13	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
14	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
15	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
16	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
17	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
18	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
19	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	

Figure 6-8 802.1X Port Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This example sets the 802.1X parameters on port 2. For a description of the additional fields displayed in this example, see "show dot1x" on page 22-41.

```
Console(config)#interface ethernet 1/2                          25-2
Console(config-if)#dot1x port-control auto                      22-36
Console(config-if)#dot1x re-authentication                      22-39
Console(config-if)#dot1x max-req 5                              22-36
Console(config-if)#dot1x timeout quiet-period 40                22-39
Console(config-if)#dot1x timeout re-authperiod 5                22-40
Console(config-if)#dot1x timeout tx-period 40                   22-41
Console(config-if)#end
Console#show dot1x                                              22-41

Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode              Authorized
1/1        disabled        Single-Host      ForceAuthorized     yes
1/2        enabled         Single-Host      Auto                yes
:
1/18       disabled        Single-Host      ForceAuthorized     n/a
1/19       disabled        Single-Host      ForceAuthorized     n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
reauth-enabled:       Disable
reauth-period:        3600
quiet-period:         60
tx-period:            30
supplicant-timeout:   30
server-timeout:       10
reauth-max:           2
max-req:              2
Status                Authorized
Operation mode        Single-Host
Max count             5
Port-control          Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    7

Authenticator State Machine
State                 Authenticated
Reauth Count          0

Backend State Machine
State                 Idle
Request Count         0
Identifier(Server)    6
```


Downloaded from www.Manualslib.com manuals search engine

```
Reauthentication State Machine
State                  Initialize
:
:
802.1X is disabled on port 1/19
Console#
```

Displaying 802.1X Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Table 6-2 802.1X Statistics

Parameter	Description
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

Downloaded from www.Manualslib.com manuals search engine

Table 6-2 802.1X Statistics (Continued)

Parameter	Description
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select Security, 802.1X, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.

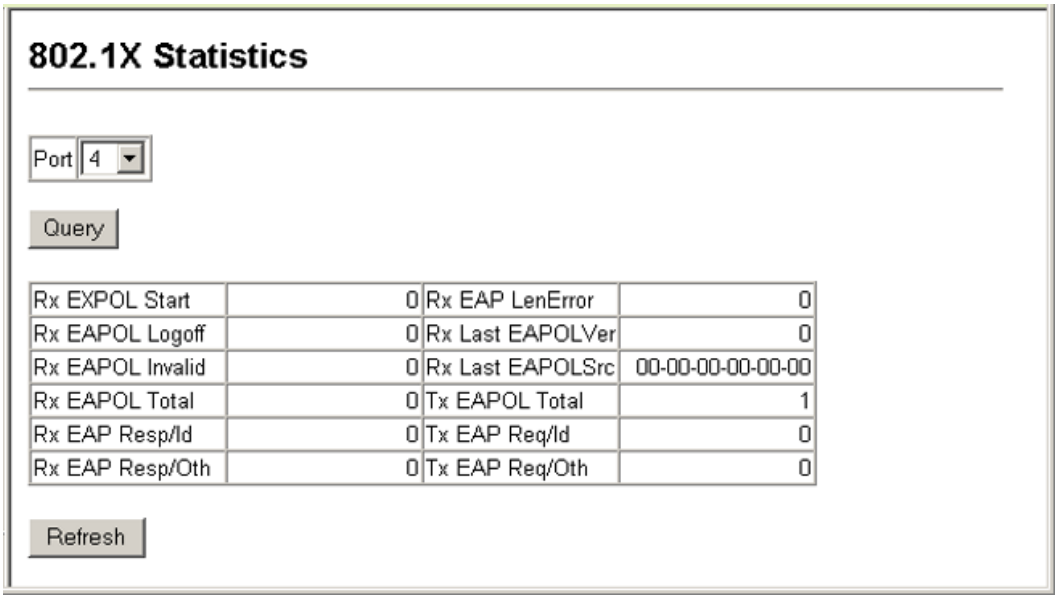


Figure 6-9 802.1X Port Statistics

CLI – This example displays the dot1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4          22-41
Eth 1/4
Rx: EAPOL      EAPOL      EAPOL      EAPOL      EAP       EAP       EAP
    Start     Logoff    Invalid    Total    Resp/Id  Resp/Oth LenError
        2          0          0       1007      672         0         0

    Last       Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL       EAP       EAP
    Total     Req/Id   Req/Oth
     2017     1005         0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Filtering IP Addresses for Management Access

You can create a list of up to 16 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

Command Usage

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **IP Filter List** – IP address which are allowed management access to this interface.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, IP Filter. Enter the IP addresses or range of addresses that are allowed management access to an interface, and click Add IP Filtering Entry.

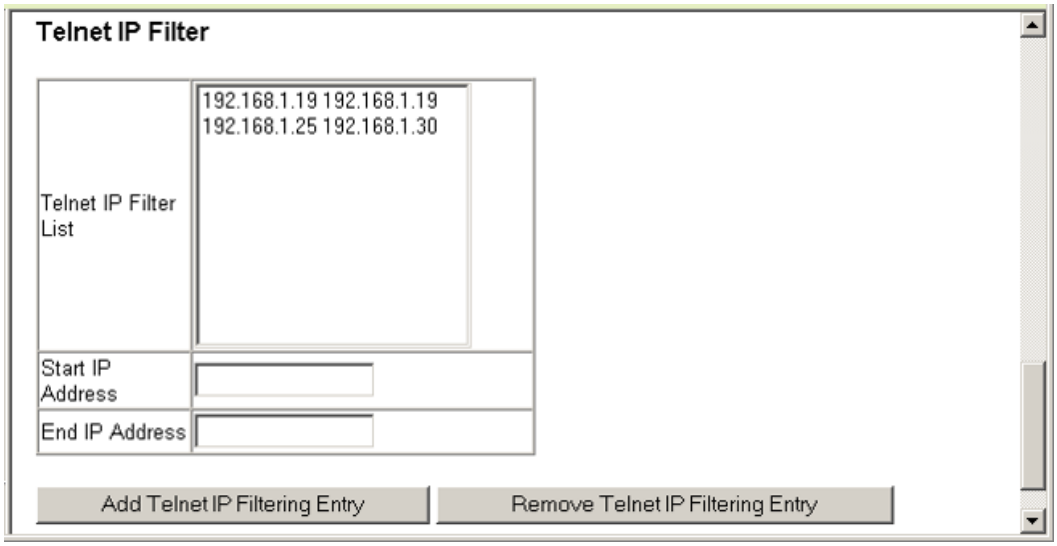


Figure 6-10 IP Filter

CLI – This example restricts management access for Telnet clients.

```
Console(config)#management telnet-client 192.168.1.19          22-45
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console(config)#exit
Console#show management all-client                              22-46
Management IP Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 7
CLIENT SECURITY

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Private VLANs and port-based authentication using IEEE 802.1X are commonly used for these purposes.

In addition to these methods, several other options of providing client security are supported by this switch. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses (either by freezing a set of dynamically learned entries or through static configuration), or to deny client access by statically configuring MAC/IP address pairs (using packet filtering rules).

DHCP service requests can be blocked to ensure that only static addresses assigned by the service provider are used, or DHCP replies can be blocked on specific ports to ensure that DHCP service requests are only answered through authorized uplink ports. The addresses assigned to DHCP clients can also be carefully controlled using dynamic bindings registered with DHCP Snooping or static bindings configured with IP Source Guard.

NetBIOS[6] traffic commonly used for resource sharing in a peer-to-peer environment can also be completely blocked to ensure that no privileged client data is passed to other data ports.

6. NetBIOS - Network Basic Input Output System

Downloaded from www.Manualslib.com manuals search engine

This switch provides client security using the following options:

- Private VLANs – Provide port-based security and isolation between ports within the assigned VLAN. (See "Configuring Private VLANs" on page 13-18.)
- 802.1X – Use IEEE 802.1X port authentication to control access to specific ports. (See "Configuring 802.1X Port Authentication" on page 6-19.)
- Port Security – Configure secure addresses for individual ports.
- IP Source Guard – Filters IP traffic on unsecure ports for which the source address cannot be identified via static source bindings nor DHCP snooping.
- DHCP Snooping – Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table.
- Packet Filtering – Filters packets with specified IP/MAC addresses, NetBIOS packets, and DHCP requests or replies.

Note: The priority of execution for the filtering commands is Port Security, Packet Filtering, IP Source Guard, and then DHCP Snooping.

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Downloaded from www.Manualslib.com manuals search engine

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (page 11-1). When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

Command Usage

- A secure port has the following restrictions:
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1 - 1024 for the port to allow access.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (page 9-4).

Command Attributes

- **Port** – Port number.
- **Name** – Descriptive text (page 25-3).
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- **Security Status** – Enables or disables port security on the port. (Default: Disabled)

Downloaded from www.Manualslib.com manuals search engine

- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
- **Trunk** – Trunk number if port is a member (page 9-9 and 9-11).

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, mark the checkbox in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port, and click Apply.

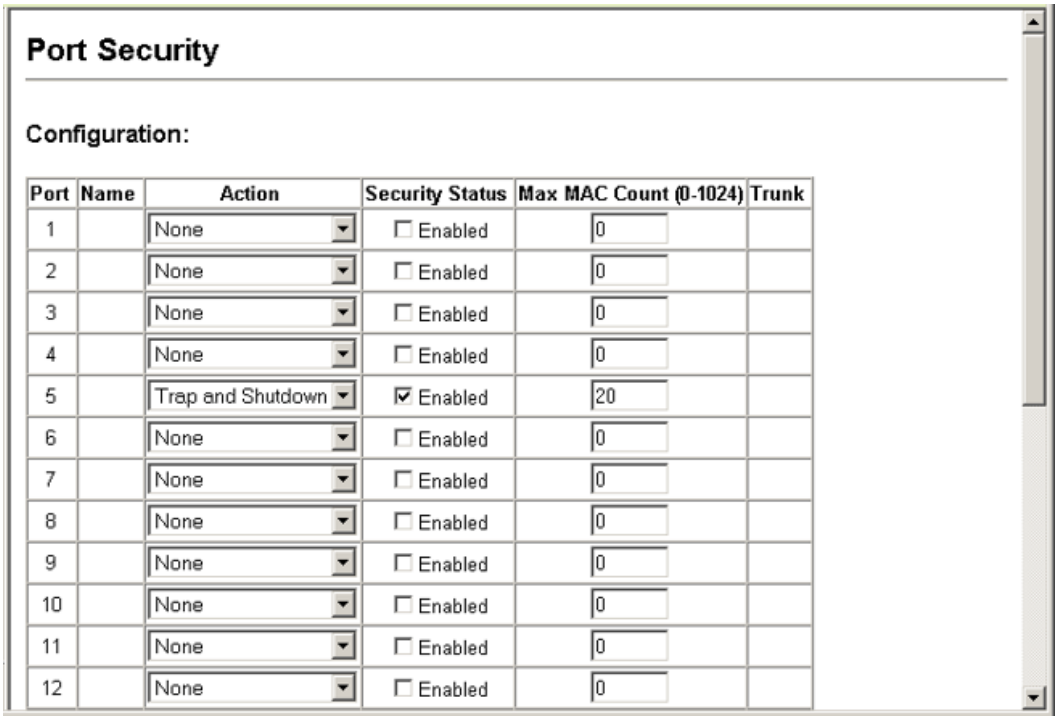

Port Security
Configuration:
Port Name Action Security Status Max MAC Count (0-1024) Trunk
1 None Enabled 0
2 None Enabled 0
3 None Enabled 0
4 None Enabled 0
5 Trap and Shutdown Enabled 20
6 None Enabled 0
7 None Enabled 0
8 None Enabled 0
9 None Enabled 0
10 None Enabled 0
11 None Enabled 0
12 None Enabled 0

Figure 7-1 Port Security

CLI – This example selects the target port, sets the port security action to send a trap and disable the port, specifies a maximum address count, and then enables port security for the port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown     23-3
Console(config-if)#port security max-mac-count 20
Console(config-if)#port security
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IP Source Guard

IP Source Guard is a security feature that filters IP traffic on unsecure network interfaces based on static entries configured in the IP Source Guard table, or dynamic entries in the DHCP Snooping table.

Command Usage

- Source guard is used to filter traffic on an unsecure port which receives messages from outside the network or firewall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- Setting source guard mode to "Source IP" or "Source IP and MAC" enables this function on the selected port. Use the "Source IP" option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the "Source IP and MAC" option to check these same parameters, plus the source MAC address.
- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping (see "Configuring DHCP Snooping" on page 7-8), or static addresses configured in the source guard binding table.
- Static addresses entered in the source guard binding table are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself, static entries include a manually configured lease time.
- Static bindings are processed as follows:
  - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type "static IP source guard binding."
  - If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
  - If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Downloaded from www.Manualslib.com manuals search engine

- If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:
  - If the DHCP snooping is disabled (see page 21-13), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
  - If IP source guard if enabled on an interface for which IP source bindings have not yet been configured (neither by static configuration in the IP source guard binding table nor dynamically learned from DHCP snooping), the switch will drop all IP traffic on that port, except for DHCP packets.

Command Attributes

IP Source Guard Binding

- **Binding Counts** – The number of static binding entries in the table.
- **Current Binding Table** – All static entries in the binding table.
- **Port** – The port to which a staic entry is bound.
- **MAC Address** – A valid unicast MAC address.
- **VLAN** – ID of a configured VLAN (Range: 1-4094)
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

Downloaded from www.Manualslib.com manuals search engine

IP Source Guard Filter

- **Port** – Port for which to filter static entries.
- **Source IP** – Filters traffic based on IP addresses stored in the binding table.
- **Source IP and MAC** – Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Web – Click IP Source Guard, Configuration. In the IP Source Guard Binding Table, select the VLAN and port to which the entry will be bound, enter the MAC address and associated IP address, then click Add Static Address. In the IP Source Guard Filter Table, select the filtering type, and then click Apply.

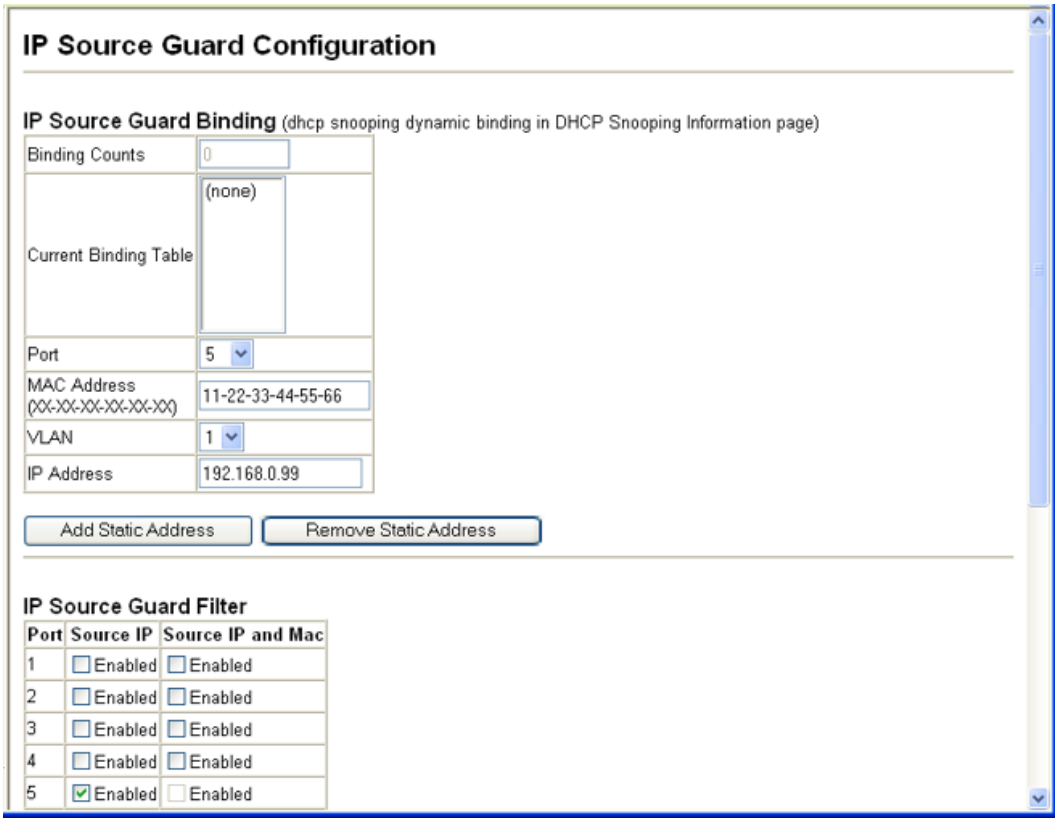


Figure 7-2 IP Source Guard Binding

Downloaded from www.Manualslib.com manuals search engine

CLI – This example configures a static source-guard binding on port 1.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1
  192.168.0.99 interface ethernet 1/5                          23-14
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip                         23-11
Console(config)#
```

Configuring DHCP Snooping

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or firewall. When DHCP snooping is enabled globally on the switch, and on a specific VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table are dropped.
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- The rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

Downloaded from www.Manualslib.com manuals search engine

- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Filtering rules are implemented as follows:
  - If the DHCP snooping is disabled globally, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
    * If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
    * If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
    * If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
    * If the DHCP packet is not a recognizable type, it is dropped.
  - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
  - If a DHCP packet from a DHCP server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

Downloaded from www.Manualslib.com manuals search engine

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Command Attributes

- **DHCP Snooping Status** – Enables DHCP snooping globally. (Default: Disabled)
- **DHCP Snooping VLAN Status** – Enables DHCP snooping on the specified VLAN. (Default: Disabled)
  - When DHCP snooping enabled globally on the switch, and enabled on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
  - When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
  - When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.
- **DHCP Snooping Verify MAC Address** – Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)
- **DHCP Snooping Database Write to Flash** – Writes all dynamically learned snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Downloaded from www.Manualslib.com manuals search engine

- **DHCP Snooping Service Provider Mode** – Once an IP address is assigned to the host by a DHCP server, the switch sets this entry to static mode in the MAC address table, and registers the host as a valid entry in the DHCP snooping table. (Default: Disabled)
  - This function applies to all VDSL ports. When set, it will automatically convert an address assigned to an attached CPE by a DHCP server to a static entry in the MAC address table. The MAC address, IP address, lease time, VLAN identifier, and port identifier are stored in the DHCP snooping table as a valid entry.
  - If the lease time assigned by the DHCP server expires, or the connection between the switch and CPE is broken for any reason, the entry will be reset to a dynamic state.
- **Trust Status** – Configures the specified interface as trusted. (Default: Untrusted)
  - A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
  - When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
  - When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- **Client Limit** – Limits the number of host devices which can be attached to a VDSL port. (Range: 1-48: Default: 5)

  The switch will monitor messages sent from a DHCP server to the attached hosts. Once the number of addresses assigned by the DHCP server reaches the client limit for an interface, no additional entries will be stored in the DHCP snooping table, and any subsequent acknowledgement packets sent by the DHCP server in response to host requests will be blocked by the switch.

Downloaded from www.Manualslib.com manuals search engine

Web – Click DHCP Snooping, DHCP Snooping Configuration. Enable DHCP snooping status globally, enable it for the required VLANs, select whether or not to verify the client's MAC address, configure those ports that will receive messages only from within the local network as trusted, and then click Apply.

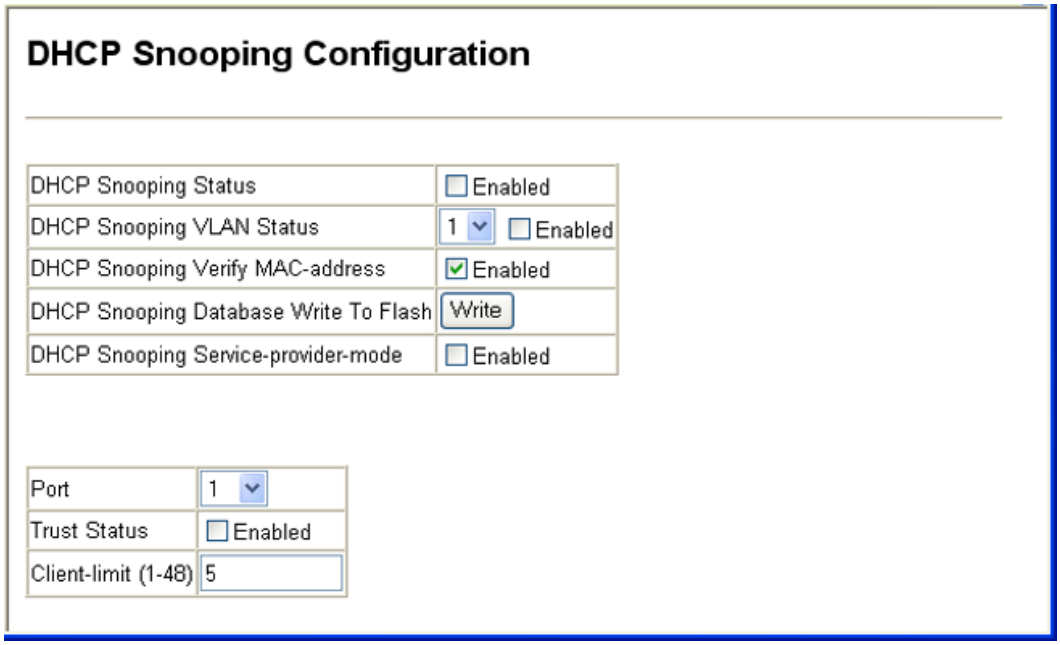


Figure 7-3 DHCP Snooping Configuration

CLI – This example enables DHCP snooping on VLAN 1, and verification of the client's MAC address. It then sets port 1 as untrusted.

```
Console(config)#ip dhcp snooping                              23-18
Console(config)#ip dhcp snooping vlan 1                       23-20
Console(config)#ip dhcp snooping verify mac-address           23-21
Console(config)#ip dhcp snooping database write               23-22
Console(config)#ip dhcp snooping service-provider-mode        23-22
Console(config)#interface ethernet 1/1
Console(config-if)#no ip dhcp snooping trust                  23-24
Console(config-if)#ip dhcp snooping client limit 48           23-23
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying DHCP Snooping Information

The configuration settings and binding table entries can be displayed on the DHCP Snooping Information page.

Command Attributes

DHCP Snooping Configuration Settings

- **DHCP Snooping Status** – DHCP snooping global configuration status.
- **DHCP Snooping Enabled VLANs** – VLANs where DHCP snooping is enabled.
- **Verify Source MAC Address** – Shows if the client's hardware address stored in the DHCP packet will be verified against the source MAC address in the Ethernet header
- **Trusted Port List** – Displays those interfaces configured as trusted. A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.

DHCP Snooping Dynamic Binding Table

- **Interface** – Switch port for which a binding entry exists.
- **VLAN** – VLAN for which DHCP snooping has been enabled.
- **MAC Address** – Physical address associated with the entry.
- **IP Address** – IP address corresponding to the client.
- **Lease** – The time for which this IP address has been leased to the client.
- **Type** – The type of binding entry. (Only Dynamic-DHCP-Binding entries are supported by this switch.)

Downloaded from www.Manualslib.com manuals search engine

Web – Click DHCP Snooping, DHCP Snooping Information.

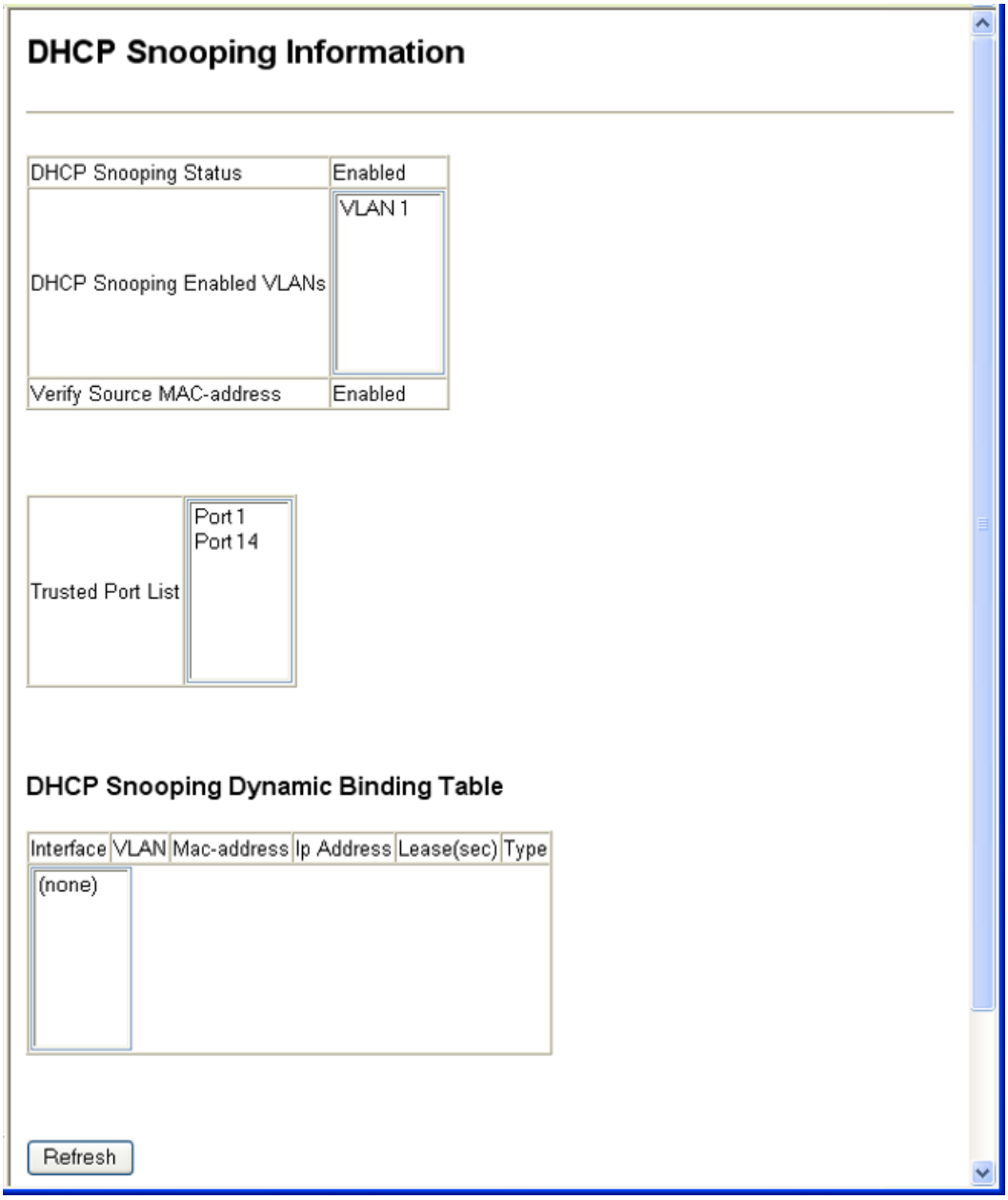


Figure 7-4 DHCP Snooping Information

Downloaded from www.Manualslib.com manuals search engine

CLI – These examples show the DHCP snooping configuration settings and binding table entries.

```
Console(config)#ip dhcp snooping                                        23-18
Console#show ip dhcp snooping                                           23-25
Global DHCP Snooping status: enable
DHCP Snooping is configured on the following VLANs:
   1,
Verify Source Mac-Address: enable
Service Provider Mode: disable
Interface           Trusted        Client-limit
----------          ----------     ------------
Eth 1/1             No             5
Eth 1/2             No             5
Eth 1/3             No             5
Eth 1/4             No             5
Eth 1/5             Yes            5
.
.
.
Console#show ip dhcp snooping binding                                   23-26
MacAddress        IpAddress       Lease(sec) Type                VLAN
Interface
----------------- --------------- ---------- -------------------- ---- --------
11-22-33-44-55-66 192.168.0.99         60000 Dynamic-DHCPSNP         1 Eth 1/5
Console#
```

Configuring Packet Filtering

Packet filtering provides security barriers between the customer and the service provider, as well as between different customers attached to the same local switch, by blocking NetBIOS traffic, DHCP service requests, and DHCP replies on specific ports.

Note: Packet Filtering occupies valuable hardware resources. Using Private VLANs provides a more efficient alternative for separating the traffic sent to each subscriber (see "Configuring Private VLANs" on page 32-17).

Filtering Service Packets

Packet filtering provides security the following security features:

- Blocking DHCP service requests to ensure that only static addresses assigned by the service provider are used.
- Blocking DHCP replies on specific ports to ensure that DHCP service requests are only answered through authorized uplink ports.

Downloaded from www.Manualslib.com manuals search engine

- Blocking NetBIOS traffic commonly used for resource sharing in a peer-to-peer environment to ensure that no privileged client data is passed to other data ports.

Command Attributes

- **DHCP Request** – Blocks DHCP request packets. (Default: Disabled)
  - In cases where the IP address for a client attached to a downlink port is fixed (i.e., at the VDSL port on the CPE), you should use this command to block any DHCP requests from the client.
  - To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
  - This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. One mask is allocated to DHCP packet filtering if enabled on any interface. This mask will be released for use by other filtering functions if DHCP packet filtering is disabled on all interfaces.
- **DHCP Reply** – Blocks DHCP reply packets. (Default: Disabled)
  - In cases where the client address is dynamically assigned by the service provider, but you need to ensure that the DHCP service reply is only obtained through an authorized uplink port, you can use this command to block DHCP replies from all unauthorized ports (commonly specifying all data ports).
  - To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
  - This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. One mask is allocated to DHCP packet filtering if enabled on any interface. This mask will be released for use by other filtering functions if DHCP packet filtering is disabled on all interfaces.

Downloaded from www.Manualslib.com manuals search engine

- **NetBIOS** – Blocks NetBIOS packets. (Default: Disabled)
  - NetBIOS is commonly used in local area networks to facilitate sharing resources such as printers or files between computers. However, when providing network services over the Internet to different customers, all information about local resources should be protected. Sending NetBIOS packets over TCP or UDP protocols can be manually disabled at the host computer. However, to ensure that this information is never sent out on the Internet, NetBIOS packet filtering should be enabled on all data ports if the switch is not operating behind a firewall.
  - When NetBIOS packet filtering is enabled, NetBIOS packets addressed to any of the TCP or UDP ports 136-139 or 445, and carrying a DSAP[7] value of 0xE0 or 0xF0, will be dropped from the specified interface.
  - To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
  - This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. Three masks are allocated to NetBIOS packet filtering if enabled on any interface. These masks will be released for use by other filtering functions if NetBIOS packet filtering is disabled on all interfaces.

7. DSAP - Destination Server Access Point; i.e., a session service tag

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, Packet Filter, Base Filter Configuration. Select the type of service packets to filter, and click Apply.

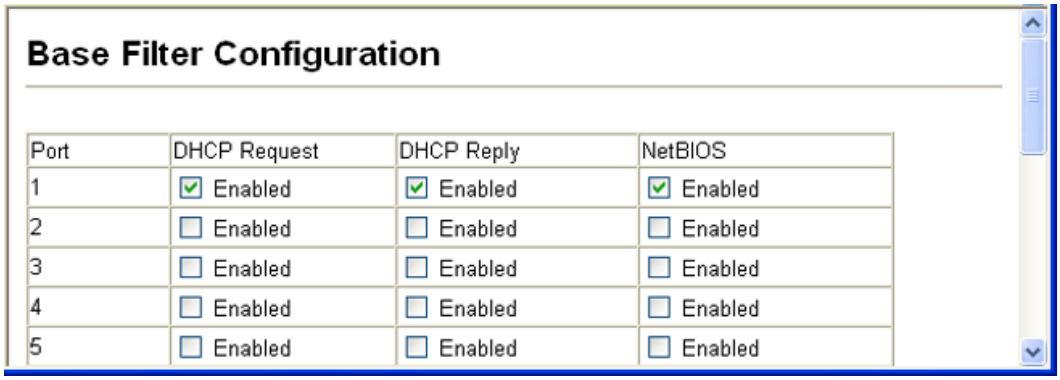


Figure 7-5 Packet Filtering – Base Filter

CLI – This example blocks DHCP service requests, DHCP reply packets, and all NetBIOS packets on port 1.

```
Console(config)#filter dhcp-request add 1/1                    23-8
Console(config)#filter dhcp add 1/1                            23-9
Console(config)#filter netbios add 1/1                         23-7
Console(config)#
```

Filtering IP/MAC Address Pairs

Packet filtering can also be used to deny network access to clients using a specified MAC/IP address pair.

Command Usage

- Both the specified source MAC address and source IP address for an entry must be matched to satisfy the filtering rule. Any packet matching a specified entry is dropped at the input port.
- To delete an entry for a MAC and IP address pair, you can specify either the MAC address or both the MAC and IP address.
- To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
- To specify a MAC address use either of the following hexidecimal formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

Downloaded from www.Manualslib.com manuals search engine

- This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. One mask is allocated to IP-MAC packet filtering if any entries are defined. This mask will be released for use by other filtering functions if all IP-MAC packet filtering entries are deleted.

Command Attributes

- **Port** – A downlink or uplink port. (Range: 1-18)
- **IP** – IP address of source.
- **MAC** – Physical address of source.

Web – Click Security, Packet Filter, IP-MAC Filter Configuration. Specify the set of IP/MAC address pairs to block, and click Add.

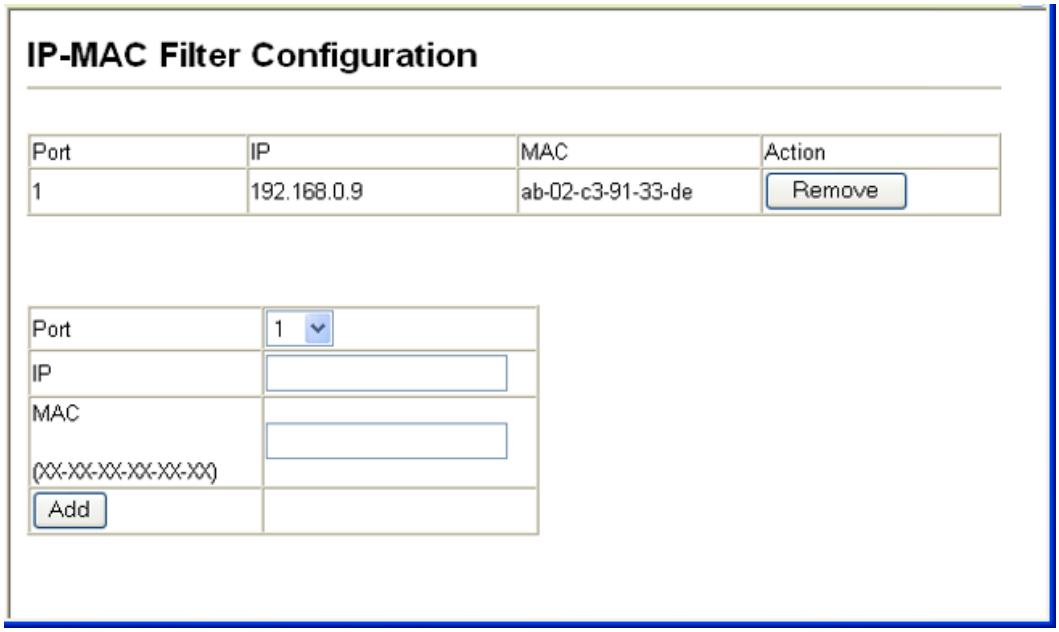


Figure 7-6 Packet Filtering – IP/MAC Filter

CLI – This example blocks all packets coming from any device attached to port 1 using the specified source IP/MAC address pair.

```
Console(config)#filter ipmac add 1/1 ab-02-c3-91-33-de
  192.168.0.9                                          23-5
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 8
ACCESS CONTROL LISTS

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule. This is done by specifying masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (that is, Ingress IP ACL, Egress IP ACL, Ingress MAC ACL, or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Downloaded from www.Manualslib.com manuals search engine

The following filtering modes are supported:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, packets can also be filtered based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Command Usage

The following restrictions apply to ACLs:

- The switch supports ACLs for both ingress and egress filtering. However, only one IP ACL and one MAC ACL can be bound to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The maximum number of ACLs is:
  Fast Ethernet ports - 157 rules, 4 masks shared by 8-port groups
  Gigabit Ethernet ports - 29 rules, 4 masks
- Each ACL can have up to 32 rules. However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Downloaded from www.Manualslib.com manuals search engine

- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
  - **Standard**: IP ACL mode that filters packets based on the source IP address.
  - **Extended**: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the "TCP" protocol is specified, then you can also filter packets based on the TCP control code.
  - **MAC**: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.

Figure 8-1 Selecting ACL Type

CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill                    24-3
Console(config-std-acl)#
```

Configuring a Standard IP ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **IP Address** – Source IP address.
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Downloaded from www.Manualslib.com manuals search engine

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Then click Add.

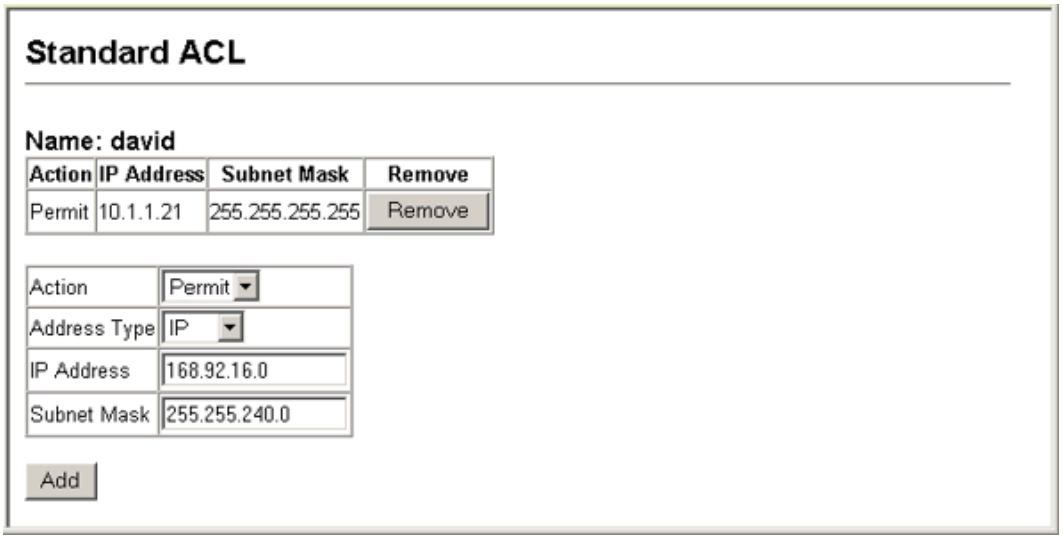


Figure 8-2 ACL Configuration - Standard IP

CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21                    24-4
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.

Downloaded from www.Manualslib.com manuals search engine

- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 8-4.)
- **Service Type** – Packet priority settings based on the following criteria:
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **TOS** – Type of Service level. (Range: 0-15)
  - **DSCP** – DSCP priority level. (Range: 0-63)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match.

  The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use control-code 2, control bitmask 2
  - Both SYN and ACK valid, use control-code 18, control bitmask 18
  - SYN valid and ACK invalid, use control-code 2, control bitmask 18

Downloaded from www.Manualslib.com manuals search engine

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.

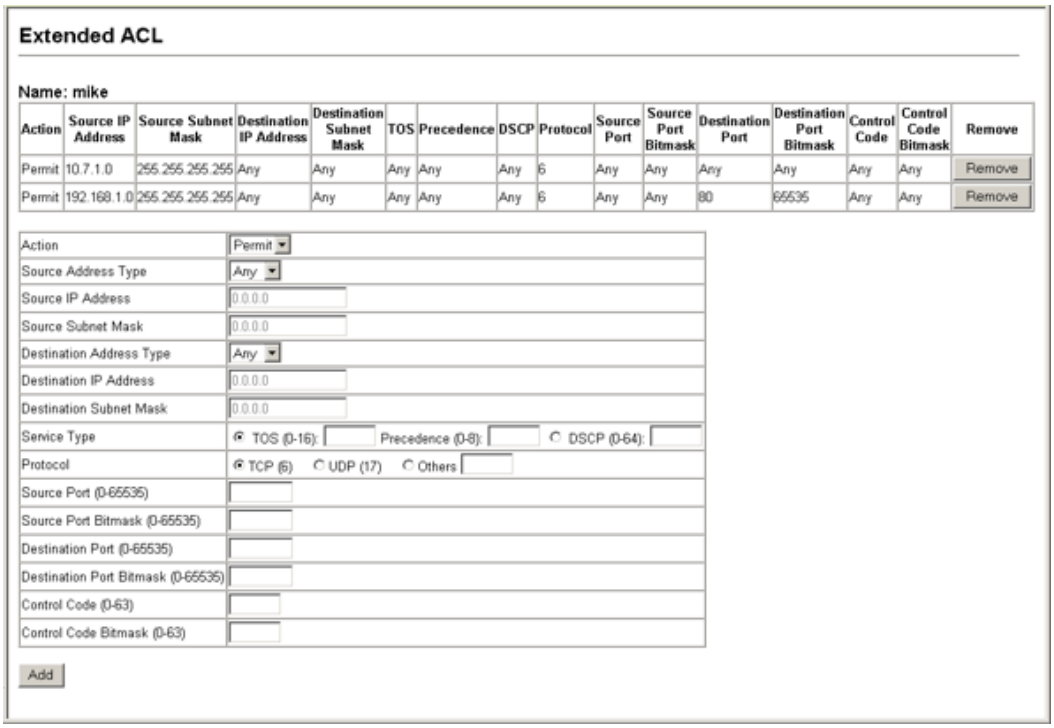


Figure 8-3 ACL Configuration - Extended IP

CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

Downloaded from www.Manualslib.com manuals search engine

3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any   24-5
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-std-acl)#
```

Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination** Address Type – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination MAC Bit Mask** – Hexidecimal mask for source or destination MAC address.
- **VID** – VLAN ID. (Range: 1-4093)
- **VID Bit Mask** – VLAN bitmask. (Range: 1-4093)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bit Mask** – Protocol bitmask. (Range: 600-fff hex.)
- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **Tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Downloaded from www.Manualslib.com manuals search engine

Command Usage

Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexidecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.

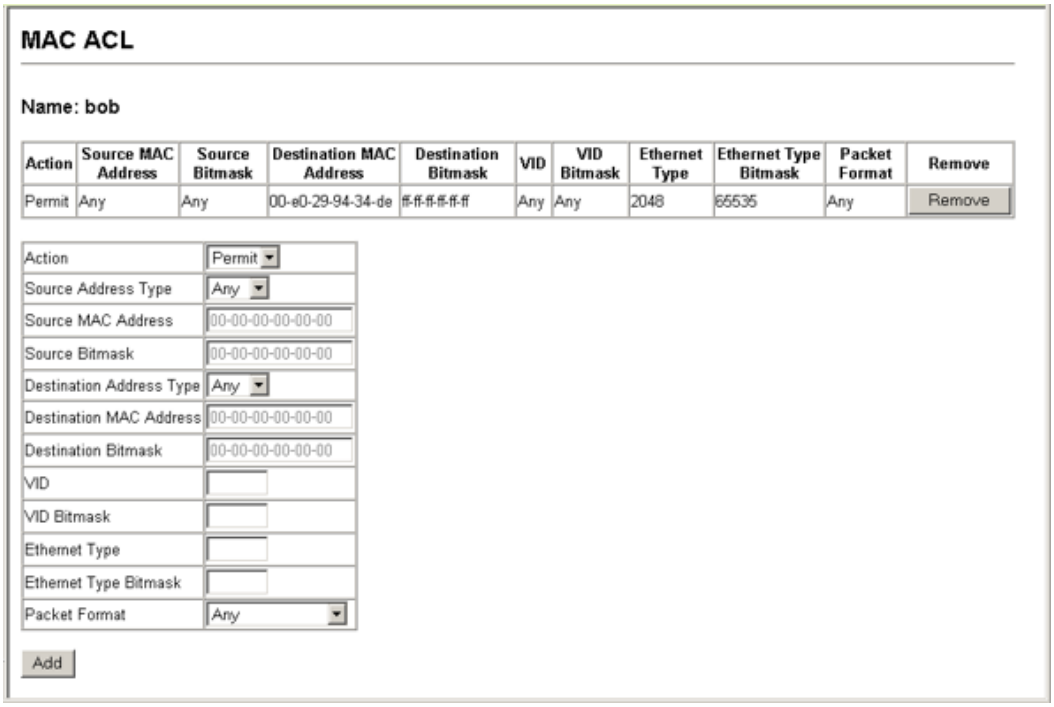


Figure 8-4 ACL Configuration - MAC

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
  ethertype 0800                                              24-18
Console(config-mac-acl)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring ACL Masks

You must specify masks that control the order in which ACL rules are checked. ACL rules matching the first entry in the mask are checked first. Rules matching subsequent entries in the mask are then checked in the specified order.

The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Usage

- Up to seven entries can be assigned to an ACL mask.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- First create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Specifying the Mask Type

Use the ACL Mask Configuration page to edit the mask for the Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Security, ACL, Mask Configuration. Click Edit for one of the basic mask types to open the configuration page.

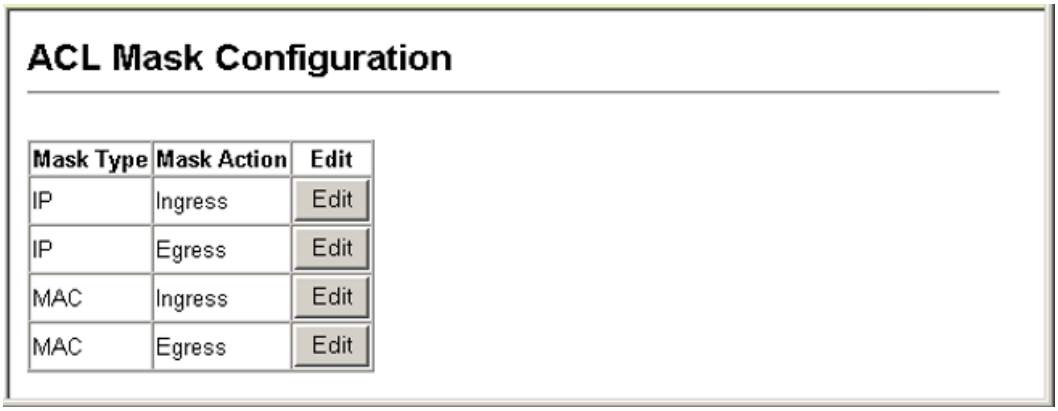


Figure 8-5 Selecting ACL Mask Types

CLI – This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in              24-8
Console(config-ip-mask-acl)#mask host any                      24-9
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Command Usage

Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to match any address, "Host" to specify a host address (not a subnet), or "IP" to specify a range of addresses. (Options: Any, Host, IP; Default: Any)

Downloaded from www.Manualslib.com manuals search engine

- **Source/Destination Subnet Mask** – Source or destination address of rule must match this bitmask. (See the description for SubMask on page 8-4.)
- **Protocol Mask** – Check the protocol field.
- **Service Type Mask** – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)
- **Source/Destination Port Bit Mask** – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **Control Code Bit Mask** – Control flags of rule must match this bitmask. (Range: 0-63)

Downloaded from www.Manualslib.com manuals search engine

Web – Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.

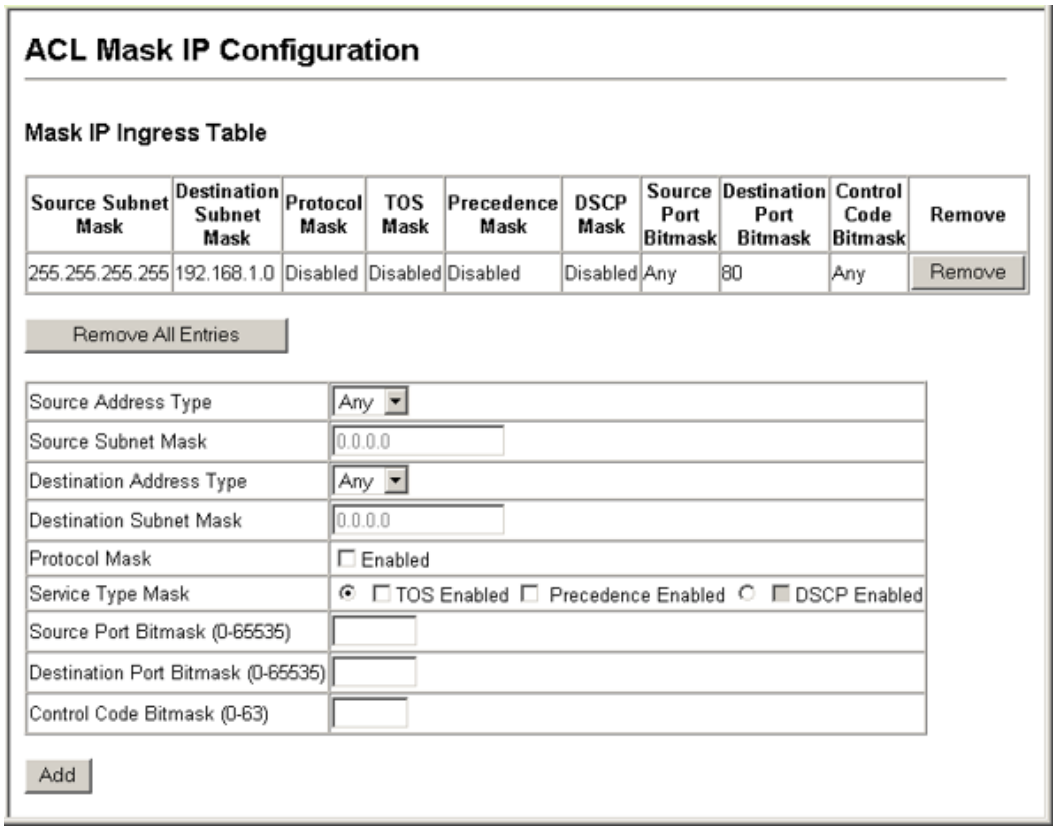


Figure 8-6 ACL Mask Configuration - IP

Downloaded from www.Manualslib.com manuals search engine

CLI – This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the "deny 10.1.1.1 255.255.255.255" rule has the higher precedence according to the "mask host any" entry.

```
Console(config)#access-list ip standard A2                    24-3
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0         24-4
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in             24-8
Console(config-ip-mask-acl)#mask host any                     24-9
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Command Usage

You must configure a mask for an ACL rule before you can bind it to a port.

Command Attributes

- **Source/Destination Address Type** – Use "Any" to match any address, "Host" to specify the host address for a single node, or "MAC" to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination Bit Mask** – Address of rule must match this bitmask.
- **VID Bitmask** – VLAN ID of rule must match this bitmask.
- **Ethernet Type Bit Mask** – Ethernet type of rule must match this bitmask.
- **Packet Format Mask** – A packet format must be specified in the rule.

Downloaded from www.Manualslib.com manuals search engine

Web – Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for specific VLAN ID(s) or Ethernet type(s). Or check for rules where a packet format was specified. Then click Add.

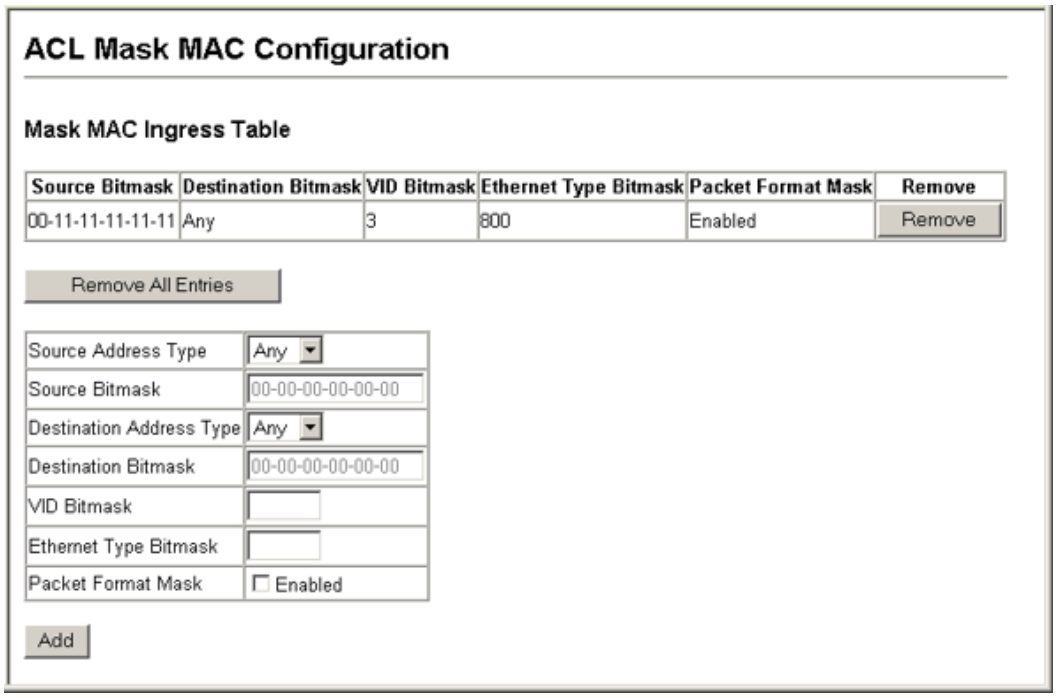


Figure 8-7 ACL Mask Configuration - MAC

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4                                  24-17
Console(config-mac-acl)#permit any any                              24-18
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
  ff-ff-ff-ff-ff-ff any vid 3                                       24-18
Console(config-mac-acl)#end
Console#show access-list                                            24-26
MAC access-list M4:
   permit any any
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in                  24-20
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff
  any vid                                                           24-21
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12                             25-2
Console(config-if)#mac access-group M4 in                           24-25
Console(config-if)#end
Console#show access-list
MAC access-list M4:
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
   permit any any
MAC ingress mask ACL:
   mask pktformat host any vid
Console#
```

Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you should bind them to the ports that need to filter traffic. You can only bind a port to one ACL for each basic type – IP ingress, IP egress, MAC ingress and MAC egress.

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port.
- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.

Downloaded from www.Manualslib.com manuals search engine

- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit "deny any any" rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

- **Port** – Fixed port or SFP module. (Range: 1-19)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IN** – ACL for ingress packets.
- **OUT** – ACL for egress packets. (Egress filtering is not supported.)
- *ACL Name* – Name of the ACL.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress traffic, select the required ACL from the drop-down list, then click Apply.

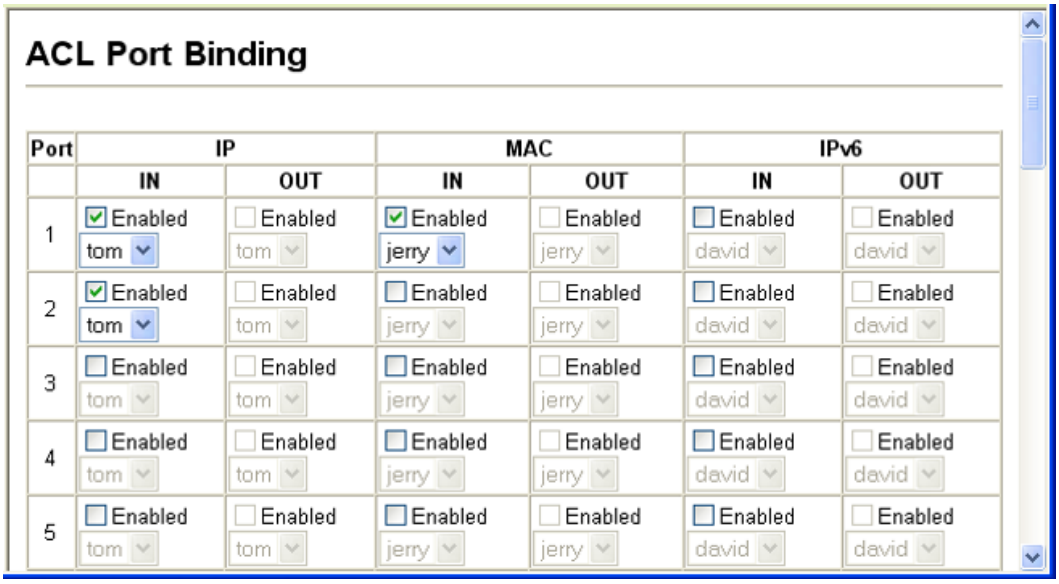

ACL Port Binding
Port
IP
MAC
IPv6
IN
OUT
IN
OUT
IN
OUT
1 Enabled tom Enabled tom Enabled jerry Enabled jerry Enabled david Enabled david
2 Enabled tom Enabled tom Enabled jerry Enabled jerry Enabled david Enabled david
3 Enabled tom Enabled tom Enabled jerry Enabled jerry Enabled david Enabled david
4 Enabled tom Enabled tom Enabled jerry Enabled jerry Enabled david Enabled david
5 Enabled tom Enabled tom Enabled jerry Enabled jerry Enabled david Enabled david

Figure 8-8 ACL Port Binding

Downloaded from www.Manualslib.com manuals search engine

CLI – This examples assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config-if)#ip access-group tom in                       24-14
Console(config-if)#mac access-group jerry in                    24-25
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group tom in
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 9
PORT CONFIGURATION

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Flow Control Status** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Media Type**[8] – Shows the forced/preferred port type to use for combination ports 17-18. (Copper-Forced, SFP-Forced, SFP-Preferred-Auto)
- **Trunk Member**[8] – Shows if port is a trunk member.
- **Creation**[9] – Shows if a trunk is manually configured or dynamically set via LACP.

8. Port Information only.
9. Trunk Information only.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Port Information or Trunk Information.

Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1		100Base-TX	Enabled	Down	100full	None	Disabled	None	
2		100Base-TX	Enabled	Down	100full	None	Disabled	None	
3		100Base-TX	Enabled	Down	100full	None	Disabled	None	
4		100Base-TX	Enabled	Down	100full	None	Disabled	None	
5		100Base-TX	Enabled	Down	100full	None	Disabled	None	
6		100Base-TX	Enabled	Down	100full	None	Disabled	None	
7		100Base-TX	Enabled	Down	100full	None	Disabled	None	
8		100Base-TX	Enabled	Down	100full	None	Disabled	None	
9		100Base-TX	Enabled	Down	100full	None	Disabled	None	
10		100Base-TX	Enabled	Down	100full	None	Disabled	None	
11		100Base-TX	Enabled	Down	100full	None	Disabled	None	
12		100Base-TX	Enabled	Down	100full	None	Disabled	None	
13		100Base-TX	Enabled	Down	100full	None	Disabled	None	
14		100Base-TX	Enabled	Up	100full	None	Disabled	None	
15		100Base-TX	Enabled	Down	100full	None	Disabled	None	
16		100Base-TX	Enabled	Down	100full	None	Disabled	None	
17		1000Base-TX	Enabled	Down	1000full	None	Enabled	SFP-Preferred-Auto	
18		1000Base-TX	Enabled	Down	1000full	None	Enabled	SFP-Preferred-Auto	

Figure 9-1 Port - Port Information

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (100BASE-TX, 1000BASE-T, SFP)
- **MAC address** – The physical layer address for this port. (To access this item on the web, see "Setting the Switch's IP Address" on page 4-11.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see

Downloaded from www.Manualslib.com manuals search engine

"Configuring Interface Connections" on page 3-48.) The following capabilities are supported.

- **10half** - Supports 10 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **1000full** - Supports 1000 Mbps full-duplex operation
- **Sym** - Transmits and receives pause frames for flow control
- **FC** - Supports flow control

- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast storm limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port security** – Shows if port security is enabled or disabled.
- **Max MAC count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 1024 addresses)
- **Port security action** – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)
- **Media type** – Shows the forced/preferred port type to use for combination ports 17-18. (copper forced, SFP forced, SFP preferred auto)

Current status:

- **Link status** – Indicates if the link is up or down.
- **Port operation status** – Provides detailed information on port state. (Displayed only when the link is up.).
- **Operation speed-duplex** – Shows the current speed and duplex mode.
- **Flow control type** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or none)

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/5                    25-13
Information of Eth 1/13
 Basic information:
  Port type:               100TX
  Mac address:             00-30-F1-D4-73-A5
 Configuration:
  Name:
  Port admin:              Up
  Speed-duplex:            100full
  Capabilities:            100full
  Broadcast storm:         Enabled
  Broadcast storm limit:   500 packets/second
  Flow control:            Disabled
  LACP:                    Disabled
  Port security:           Disabled
  Max MAC count:           0
  Port security action:    None
  Media type:              None
 Current status:
  Link Status:             Up
  Port Operation Status:   Up
  Operation speed-duplex:  100full
  Flow control type:       None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed and duplex mode, and flow control.

Command Usage

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed.
- When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the

Downloaded from www.Manualslib.com manuals search engine

required operation modes must be specified in the capabilities list for an interface.

- Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode (i.e., with auto-negotiation disabled).

  Note: VDSL ports 1-16 are fixed at 100Mbps, full duplex.
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, duplex mode, and flow control. The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1 Gbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current switch chip only supports symmetric pause frames.*)
  - **FC** - Supports flow control

    Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation

Downloaded from www.Manualslib.com manuals search engine

and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

(Default: Autonegotiation is permanently disabled on ports 1-16, and enabled on ports 17-19; Advertised capabilities for
RJ-45: 100BASE-TX (Port 19) – 10half, 10full, 100half, 100full;
1000BASE-T – 10half, 10full, 100half, 100full, 1000full;
SFP: 1000BASE-SX/LX/LH – 1000full when a module is installed)

- **Media Type** – Shows the forced/preferred port type to use for the combination ports. (Ports 17-18)
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port (even if module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default.)
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see "Creating Trunk Groups" on page 9-8.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.

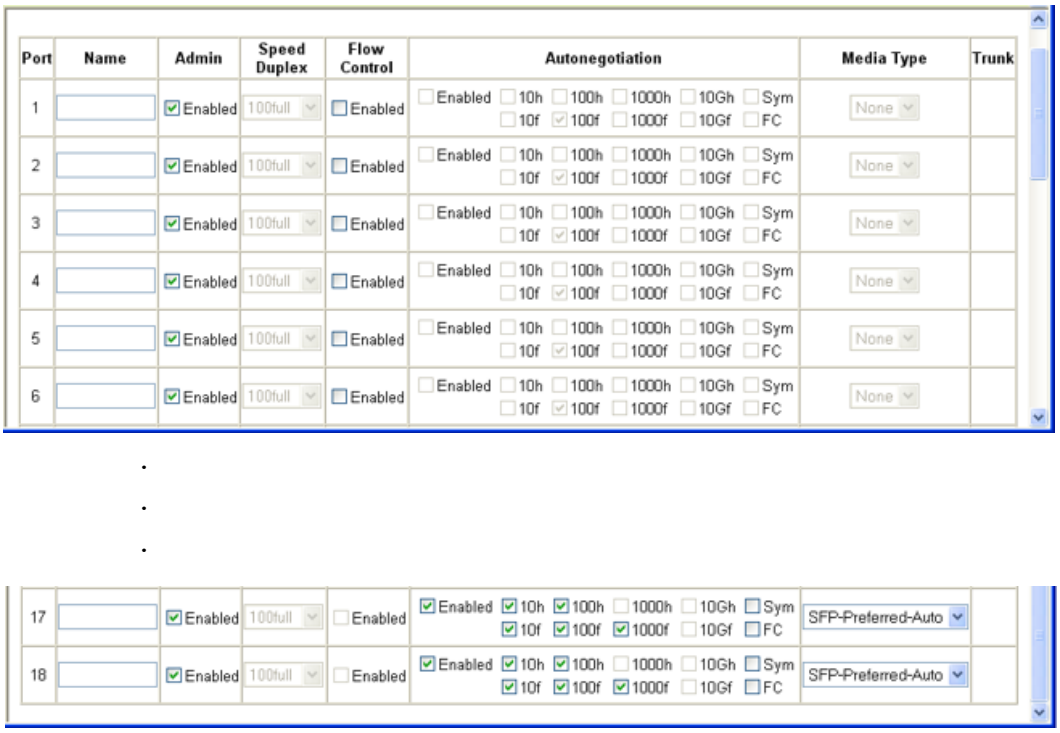

Port
Name
Admin
Speed Duplex
Flow Control
Autonegotiation
Media Type
Trunk
1 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC None
2 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC None
3 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC None
4 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC None
5 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC None
6 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC None
17 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC SFP-Preferred-Auto
18 Enabled 100full Enabled Enabled 10h 100h 1000h 10Gh Sym 10f 100f 1000f 10Gf FC SFP-Preferred-Auto

Figure 9-2 Port - Port Configuration

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/19                    25-2
Console(config-if)#description RD SW#19                    25-3
Console(config-if)#shutdown                                25-10
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                          25-5
Console(config-if)#speed-duplex 100half                    25-3
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                    25-6
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#exit
Console(config)#interface ethernet 1/18
Console(config-if)#media-type copper-forced                25-8
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Creating Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 12 trunks.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

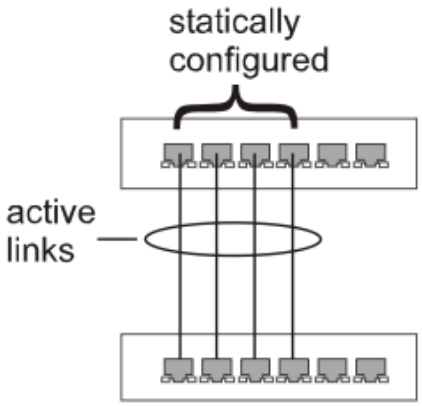
- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 12 trunks, with up to eight VDSL ports per trunk or up to two Gigabit Ethernet ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.

Downloaded from www.Manualslib.com manuals search engine

- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Statically Configuring a Trunk

Command Usage



- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

Command Attributes

- **Member List** (Current) – Shows configured trunks (Trunk ID, Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Trunk** – Trunk identifier. (Range: 1-12)
  - **Port** – Port identifier. (Range: 1-18)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Trunk Membership. Enter a trunk ID of 1-12 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.

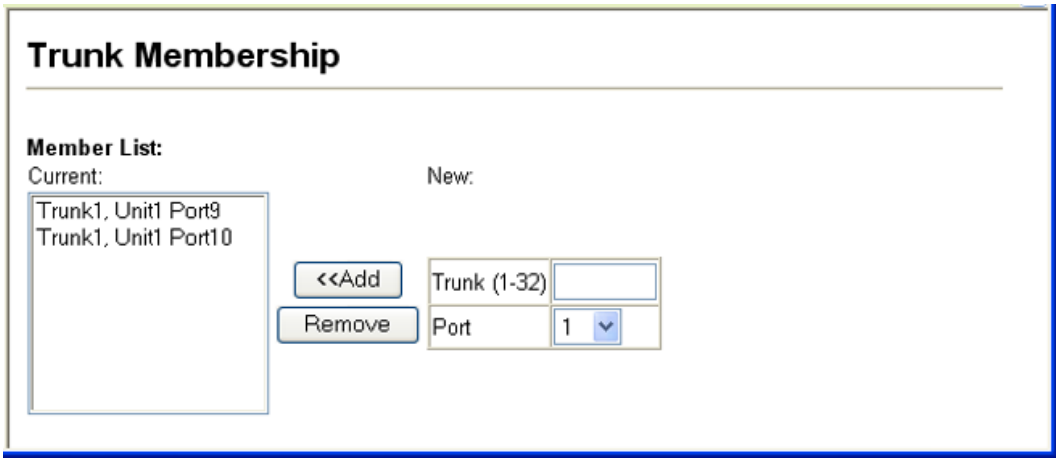


Figure 9-3 Static Trunk Configuration

Downloaded from www.Manualslib.com manuals search engine

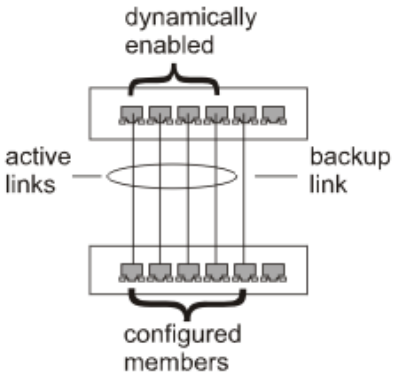
CLI – This example creates trunk 1 with ports 9 and 10. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1                    25-2
Console(config-if)#exit
Console(config)#interface ethernet 1/9                      25-2
Console(config-if)#channel-group 1                          26-3
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1               25-13
Information of Trunk 1
 Basic information:
  Port type:              100TX
  Mac address:            00-30-F1-D4-73-A2
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           100full
  Capabilities:           100full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             User
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 100full
  Flow control type:      None
  Member Ports: Eth1/9, Eth1/10,
Console#
```

Enabling LACP on Selected Ports

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.



Downloaded from www.Manualslib.com manuals search engine

- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- Trunks dynamically established through LACP will also be shown in the Member List on the Trunk Membership menu (see page 9-9).

Command Attributes

- **Member List** (Current) – Shows configured trunks (Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Port** – Port identifier. (Range: 1-18)

Web – Click Port, LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.

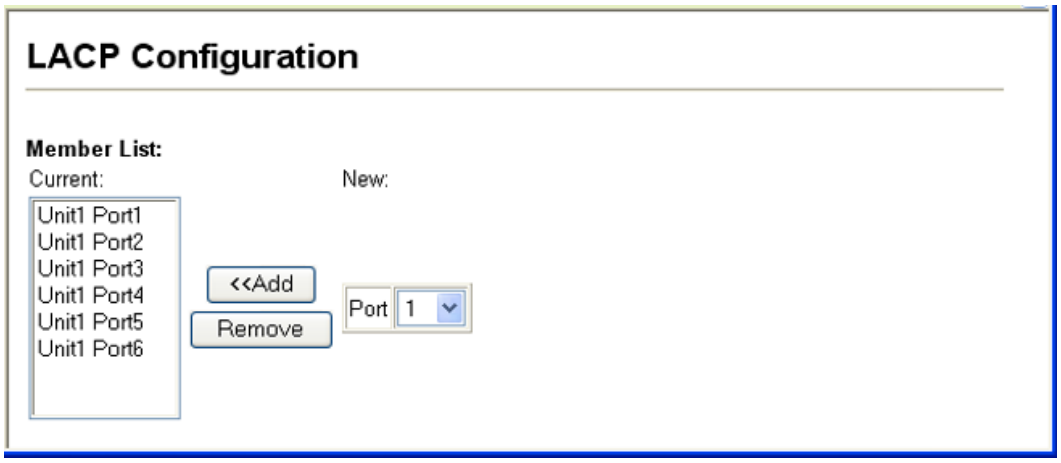


Figure 9-4 LACP Trunk Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config-if)#lacp                                         26-4
Console(config-if)#exit
⋮
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                   25-13
Information of Trunk 1
 Basic information:
  Port type:              100TX
  Mac address:            00-30-F1-D4-73-A2
 Configuration:
  Port admin:             Up
  Speed-duplex:           100full
  Capabilities:           100full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             LACP
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 100full
  Flow control type:      None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

Configuring LACP Parameters

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the "port channel" Admin Key is set (page 4-142), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

Downloaded from www.Manualslib.com manuals search engine

Note: If the port channel admin key (lacp admin key, page 26-8) is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 26-7).

Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; i.e., the ports on this switch.

- **Port** – Port number. (Range: 1-18)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
  - Ports must be configured with the same system priority to join the same LAG.
  - System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.

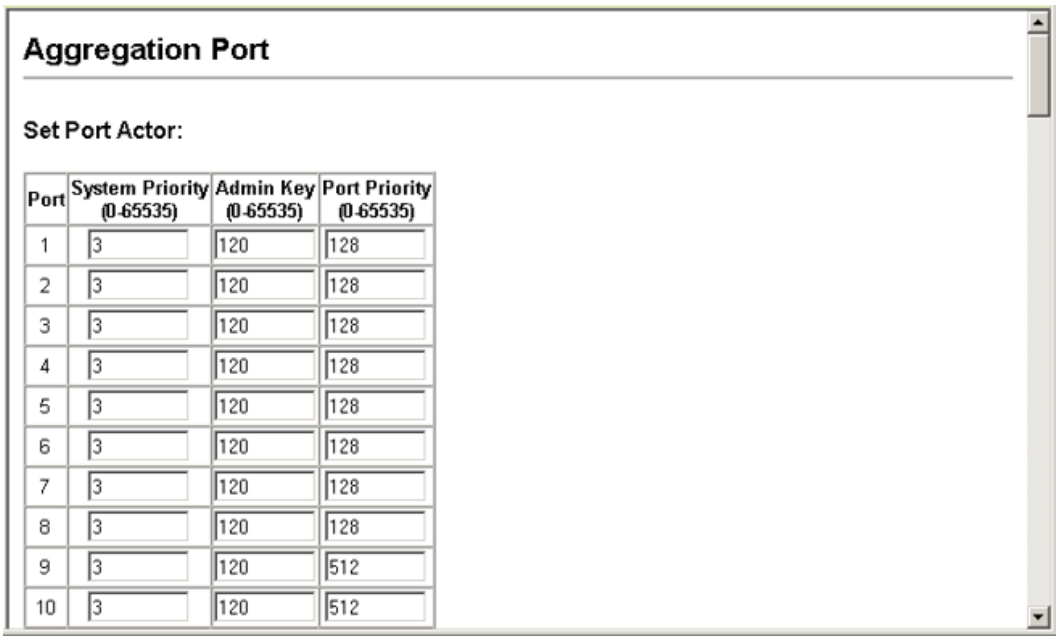


Figure 9-5 LACP - Aggregation Port

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example configures LACP parameters for ports 1-10. Ports 1-8 are used as active members of the LAG, ports 9 and 10 are set to backup mode.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config-if)#lacp actor system-priority 3                 26-6
Console(config-if)#lacp actor admin-key 120                     26-7
Console(config-if)#lacp actor port-priority 128                 26-9
Console(config-if)#exit
:
Console(config)#interface ethernet 1/10
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid                                         26-10
Channel Group    System Priority    System MAC Address
---------------------------------------------------------------------
            1                  3     00-00-E9-31-31-31
            2              32768     00-00-E9-31-31-31
            3              32768     00-00-E9-31-31-31
:
Console#show lacp 1 internal                                    26-10
Port channel: 1
---------------------------------------------------------------------
Oper Key:  120
Admin Key: 0
Eth 1/ 1
---------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 3
  LACP Port Priority:   128
  Admin Key:            120
  Oper Key:             120
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
```


Downloaded from www.Manualslib.com manuals search engine

Displaying LACP Port Counters

You can display statistics for LACP protocol messages.

Table 9-1 LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received by this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Web – Click Port, LACP, Port Counters Information. Select a member port to display the corresponding information.

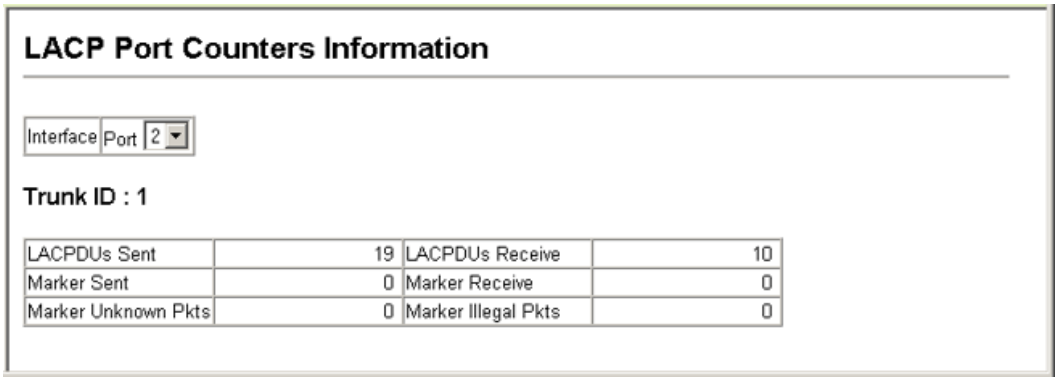

LACP Port Counters Information
Interface Port 2
Trunk ID : 1
LACPDUs Sent 19 LACPDUs Receive 10
Marker Sent 0 Marker Receive 0
Marker Unknown Pkts 0 Marker Illegal Pkts 0

Figure 9-6 LACP - Port Counters Information

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example displays LACP counters for port channel 1.

```
Console#show lacp 1 counters                                    26-10
Port channel: 1
---------------------------------------------------------------------
Eth 1/ 2
---------------------------------------------------------------------
  LACPDUs Sent:          19
  LACPDUs Receive:       10
  Marker Sent:           0
  Marker Receive:        0
  LACPDUs Unknown Pkts:  0
  LACPDUs Illegal Pkts:  0
:
```

Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

Table 9-2 LACP Internal Configuration Information

Field	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.

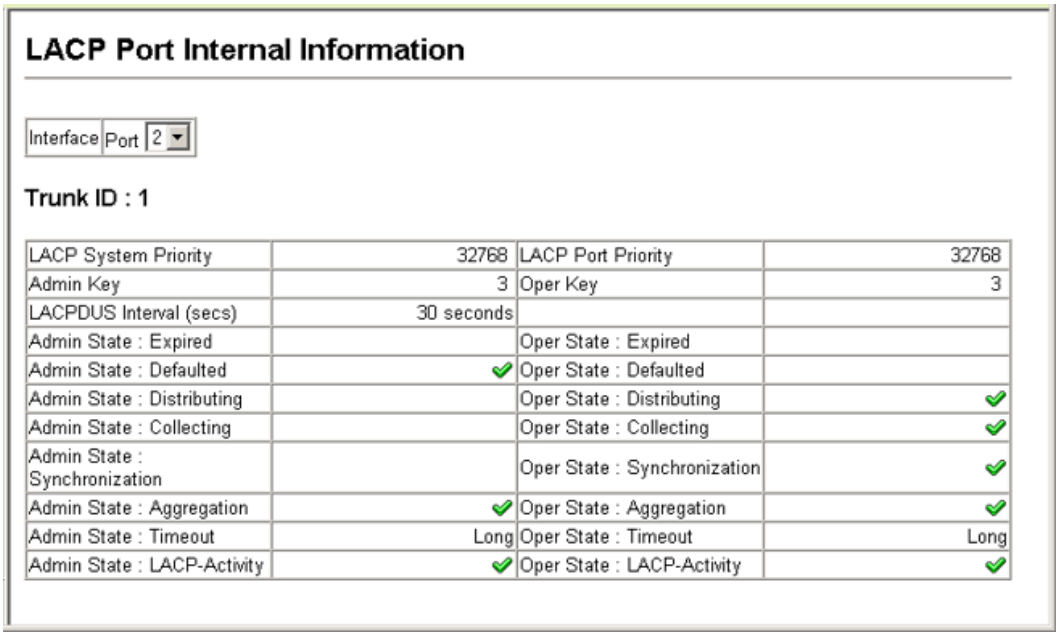
Downloaded from www.Manualslib.com manuals search engine

Table 9-2 LACP Internal Configuration Information (Continued)

Field	Description
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.



LACP Port Internal Information

Interface Port 2

Trunk ID : 1

LACP System Priority	32768	LACP Port Priority	32768
Admin Key	3	Oper Key	3
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	✓
Admin State : Collecting		Oper State : Collecting	✓
Admin State : Synchronization		Oper State : Synchronization	✓
Admin State : Aggregation	✓	Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity	✓	Oper State : LACP-Activity	✓

Figure 9-7 LACP - Port Internal Information

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show lacp 1 internal                                    26-10
Port channel: 1
------------------------------------------------------------------------
Oper Key:  3
Admin Key: 0
Eth 1/ 2
------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 32768
  LACP Port Priority:   32768
  Admin Key:            3
  Oper Key:             3
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
```


Downloaded from www.Manualslib.com manuals search engine

Displaying LACP Settings and Status for the Remote Side

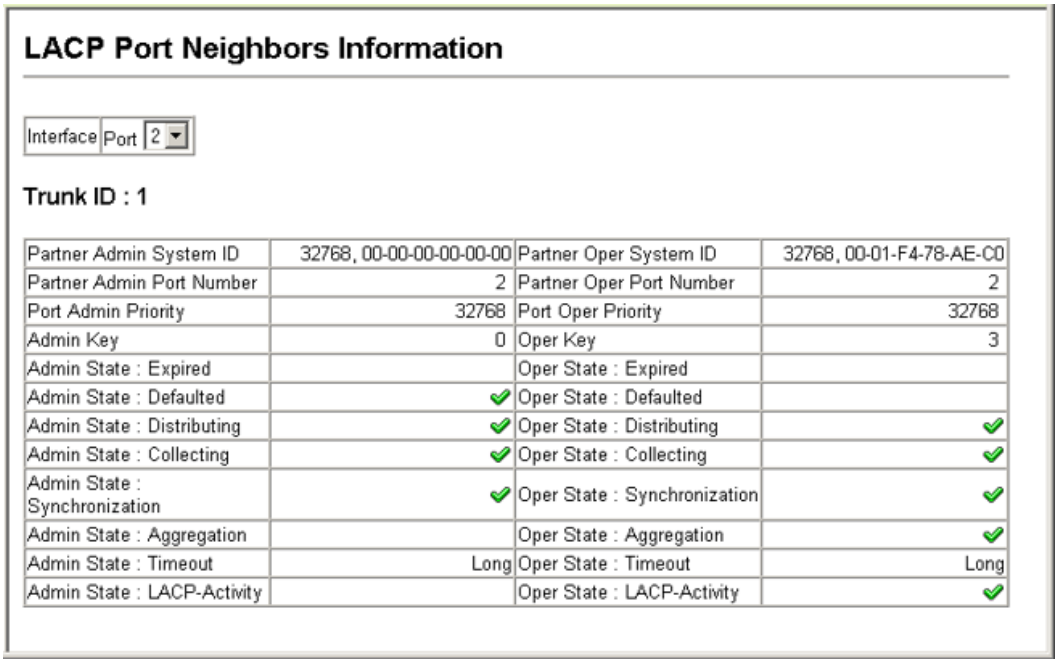
You can display configuration settings and the operational state for the remote side of an link aggregation.

Table 9-3 LACP Neighbor Configuration Information

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Interface Port 2

Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-01-F4-78-AE-C0
Partner Admin Port Number	2	Partner Oper Port Number	2
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	3
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing	✓	Oper State : Distributing	✓
Admin State : Collecting	✓	Oper State : Collecting	✓
Admin State : Synchronization	✓	Oper State : Synchronization	✓
Admin State : Aggregation		Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✓

Figure 9-8 LACP - Port Neighbors Information

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show lacp 1 neighbors                                    26-10
Port channel 1 neighbors
-------------------------------------------------------------------
Eth 1/2
-------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    32768, 00-01-F4-78-AE-C0
  Partner Admin Port Number: 2
  Partner Oper Port Number:  2
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:              distributing, collecting, synchronization,
                             aggregation, long timeout, LACP-activity
:
```


Downloaded from www.Manualslib.com manuals search engine

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

- Broadcast control does not effect IP multicast traffic.
- The resolution is 1 packet per second (pps); i.e., any setting between 500-262143 is acceptable.

Note: Multicast and unknown unicast storm thresholds can also be set using the CLI (see the "switchport packet-rate" command on page 25-11).

Command Attributes

- **Port**[10] – Port number.
- **Trunk**[11] – Trunk number
- **Type** – Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)
- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (Options: 500-262143 packets per second; Default: 500 pps)
- **Trunk**[10] – Shows if port is a trunk member.

10. Port Broadcast Control
11. Trunk Broadcast Control

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Port Broadcast Control or Trunk Broadcast Control. Check the Enabled box for any interface, set the threshold, and click Apply.

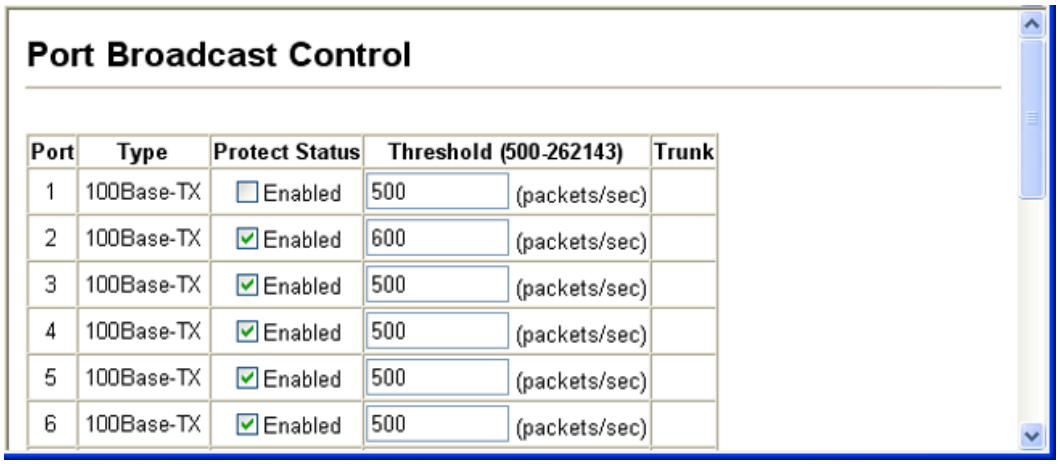


Figure 9-9 Port Broadcast Control

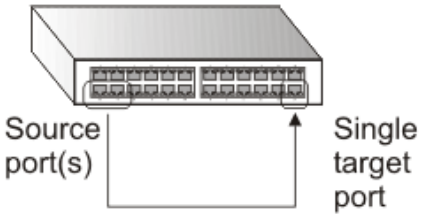
CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config-if)#no switchport broadcast                      25-11
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 600         25-11
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2                 25-16
Information of Eth 1/2
 Broadcast threshold:            Enabled, 600 packets/second
 Multicast Threshold:            Enabled, 500 packets/second
 UnknownUnicast Threshold:       Enabled, 500 packets/second
 LACP status:                    Disabled
 Ingress Rate Limit:             Disabled, 102400K bits per second
 Egress Rate Limit:              Disabled, 102400K bits per second
 Ingress Rate Limit Trap:        Disabled, Up:0 packets,Down:0
packets
 VLAN membership mode:           Hybrid
 Ingress rule:                   Disabled
 Acceptable frame type:          All frames
 Native VLAN:                    1
 Priority for untagged traffic: 0
 GVRP status:                    Disabled
 Allowed VLAN:                   1(u),
 Forbidden VLAN:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see "Spanning Tree Algorithm" on page 12-1).

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored. (Range: 1-18)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)
- **Target Port** – The port that will "mirror" the traffic from the source port. (Range: 1-18)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Mirror Port Configuration. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.

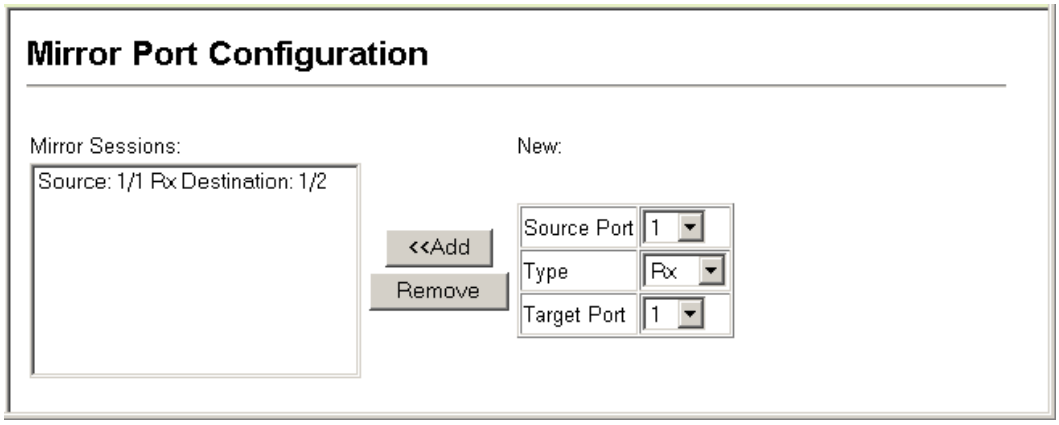


Figure 9-10 Mirror Port Configuration

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/2                    25-2
Console(config-if)#port monitor ethernet 1/1              27-1
Console(config-if)#
```

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

The rate limit may be set for both ingress and egress of any port or trunk. However, only the rate limit for ingress traffic can be controlled for a VLAN member port.

Downloaded from www.Manualslib.com manuals search engine

Note: You can also set an SNMP trap if traffic exceeds the configured rate limit using the CLI (see the "rate-limit trap-input" command on page 28-3).

Command Attribute

Rate Limit – Sets the input or output rate limit for an Ethernet interface, or the input rate limit for a VLAN port member, in increments of 64 Kbps.

Default Status: Disabled
Default Rate: 1024000 Kbps
Range: 64 - 1024000 Kbps

Configuring Rate Limits for an Ethernet Interface

Web - Click Port, Rate Limit, Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.

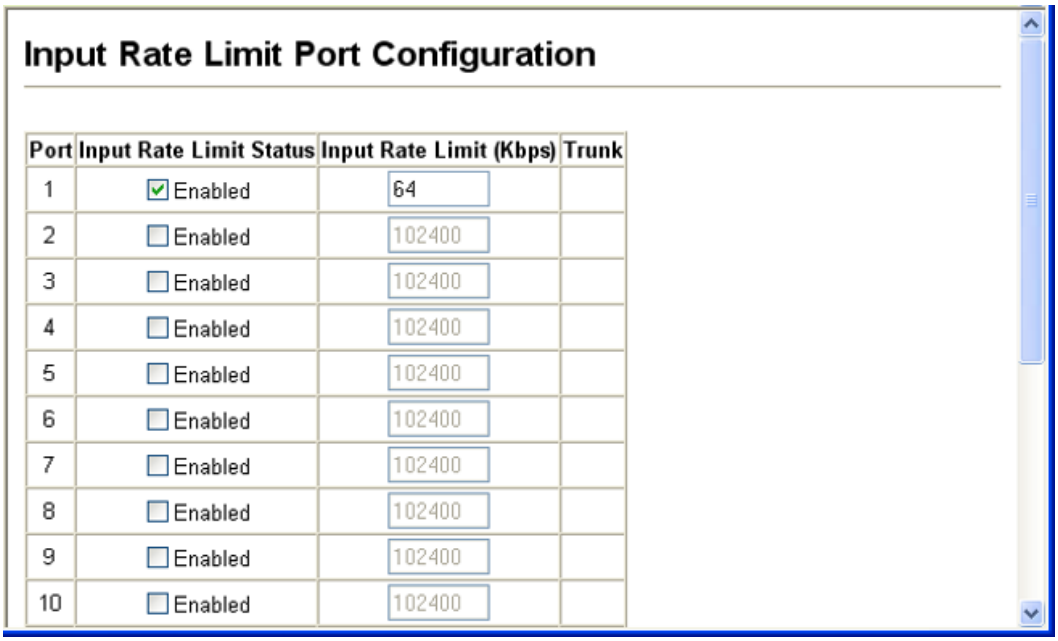


Figure 9-11 Rate Limit Configuration for Ethernet Interface

Downloaded from www.Manualslib.com manuals search engine

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 64 Kbps.

```
Console(config)#interface ethernet 1/1                    25-2
Console(config-if)#rate-limit input 64                    28-2
Console(config-if)#rate-limit output 64
Console(config-if)#
```

Configuring the Rate Limit for a VLAN Port Member

Web - Click Port, Rate Limit, Input VLAN Configuration. Select the port, and the VLAN to which the port belongs. Set the input rate limit for the selected interface, and then click Add.

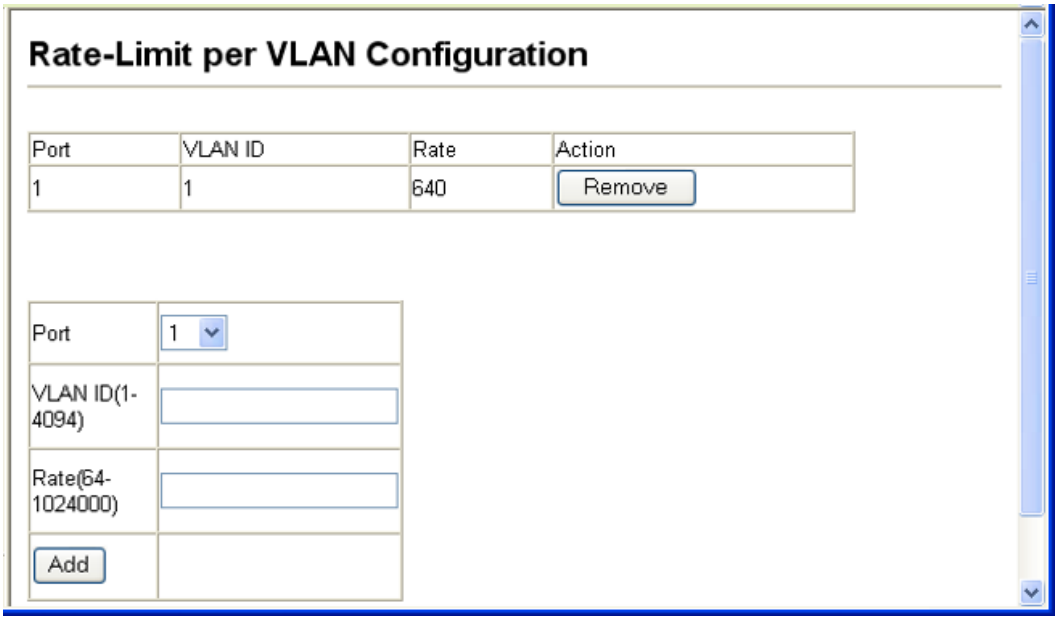


Figure 9-12 Rate Limit Configuration for VLAN Port Member

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 64 Kbps.

```
Console(config)#interface ethernet 1/1                    25-2
Console(config-if)#rate-limit vlan 1 640                  28-2
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as SMC EliteView.

Table 9-4 Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Downloaded from www.Manualslib.com manuals search engine

Table 9-4 Port Statistics (Continued)

Parameter	Description
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Downloaded from www.Manualslib.com manuals search engine

Table 9-4 Port Statistics (Continued)

Parameter	Description
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.

Downloaded from www.Manualslib.com manuals search engine

Table 9-4 Port Statistics (Continued)

Parameter	Description
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

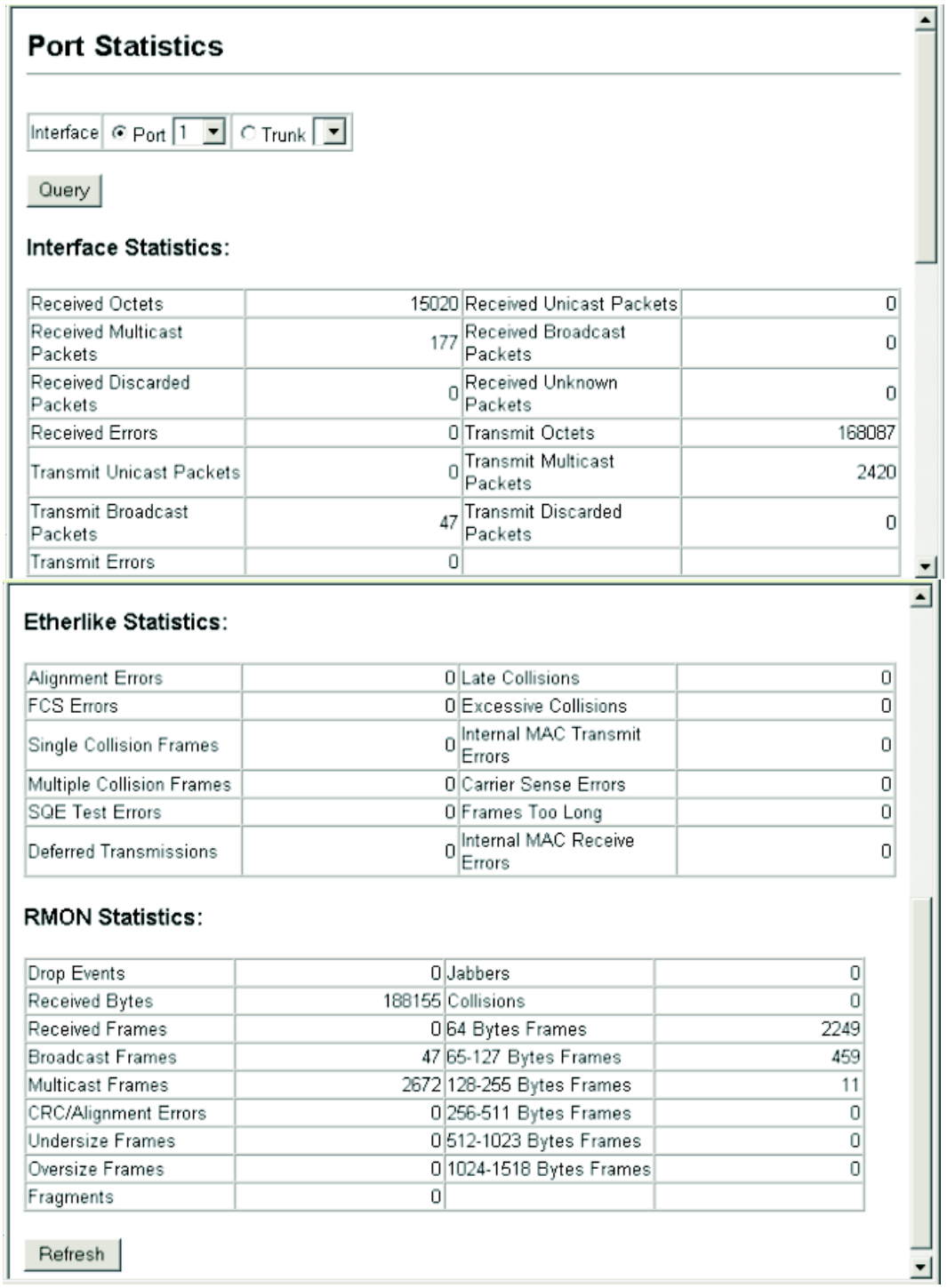
Downloaded from www.Manualslib.com manuals search engine

Table 9-4 Port Statistics (Continued)

Parameter	Description
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Downloaded from www.Manualslib.com manuals search engine

Web – Click Port, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.



Port Statistics

Interface: Port 1 / Trunk

Query

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

Figure 9-13 Port Statistics

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows statistics for port 12.

```
Console#show interfaces counters ethernet 1/12                          25-14
Ethernet 1/12
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 10
VDSL CONFIGURATION

VDSL communication parameters can be set for individual ports, or multiple parameters can be defined in a profile and applied globally to the switch or to a group of ports. Alarm thresholds can be defined in a profile and then applied globally to the switch or to selected ports. The switch also provides an extensive listing of VDSL statistics.

For intelligent CPEs, the remote device can be configured for standard Ethernet connection parameters, priority settings, and queue usage. System status and performance counters can be monitored. And firmware can be remotely upgraded.

Configuring Global Settings for VDSL Ports

This section describes how to configure communication parameters for all of the VDSL ports. These global parameters include specifying the Power Spectral Density (PSD) breakpoints and a predefined PSD mask, upstream power backoff (UPBO) and associated mask, automatic line rate adaptation, maximum input and output data rates, and automatic re-training to find the optimal transmission rate.

Command Attributes

- **PSD Breakpoints** – Define the frequency / power level breakpoints used in the Power Spectral Density (PSD) mask.
  - *Number of Breakpoints* – The number of frequency breakpoints used in the PSD mask. (Range: 0-28; Default: 28)
  - **Frequency Value** – A frequency assigned to the corresponding breakpoint. (Range: 0-30000 kHz)

Downloaded from www.Manualslib.com manuals search engine

- **Power Value** – A power level for each of the PSD breakpoints. (Range: An integer from 0 to 255, which is used to calculate a power level in terms of -140 + (*power-value*) * 0.5 dBm/Hz; Default: 255, which is equivalent to -12.5 dBm/Hz)

Breakpoints, which are defined by a signal frequency and corresponding power level, create a PSD mask for in-band spectrum shaping, set the Limit PSD Mask required for compliance with local regulations, or set mask limits for upstream power backoff. The methods used to calculate these various PSD masks, and local regulations governing the power spectrum used on VDSL lines are all described in ITU-T G.993.2.

Breakpoints can be applied to any upstream or downstream channel depending on the associated frequencies.

Note that settings for the MIB PSD mask can only be configured through an SNMP network management interface.

- **PSD Mask Level** – Sets a predefined PSD mask. (Options: See Table 29-6, "PSD Mask Options," on page 29-17; Default: 5, Annex F)
- **UPBO** – Enables upstream power backoff. (Default: Disabled)

  Upstream power backoff (UPBO) should be configured when there are VDSL connections of different lengths attached to this switch. UPBO is required to improve the spectral compatibility on lines of different lengths by reducing the transmitted power on shorter lines. If UPBO is enabled, the transceiver will use the PBO mask as defined in the UPBO Configuration table. Additional information about the power backoff PSD mask can be found in ITU-T G.992.2. If UPBO is enabled, but a PBO mask has not been configured, the specified transceiver will automatically control upstream power backoff based on default values set by the DSP engine
- **Rate Adaption** – Enables automatic line rate adaptation, which can set the optimal transmission rate based on existing line conditions. (Default: Enabled)

  The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaptation is enabled and the port links up, the switch will determine

Downloaded from www.Manualslib.com manuals search engine

the optimal transmission rate for the current conditions, setting the rate within the bounds defined by the Data Rate.

When rate adaptation is enabled and the signal quality deteriorates on any line or the link is re-established after being dropped, that port will automatically enter retraining and connect at the optimum rate if Auto-retraining is enabled (described later in this section). Otherwise, the rate can be manually retrained (see the description for Retraining under "Configuring Interface Settings for VDSL Ports" on page 10-7).

- **Rate Set** – Sets the maximum input and output data rates for the VDSL ports. (Range: 1-200,000 kbps; Default: Based on Auto-retraining if enabled, otherwise undefined)
- **Auto-retraining** – Initiates the rate adaption method to find the optimal transmission rate based on existing line conditions. (Default: Enabled)

  When auto-retraining is enabled and signal quality deteriorates on any line, that port will automatically enter retraining and connect at the optimum rate based on the bounds defined by the Date Rate defined for each VDSL port (see "Configuring Interface Settings for VDSL Ports" on page 10-7).
- **UPBO Configuration** – Sets a mask to reduce the power spectral density (PSD) of transmitted signals at specified frequency breakpoints for upstream power backoff.
  - **K1[0-5]** – Frequency breakpoints for upstream bands DS1-DS3.
  - **K2[0-5]** – Frequency breakpoints for downstream bands US0-US2.
  - **Value** – Limitation on the PSD at specified breakpoint. (Range: -1000000 to 1000000, in units of 1000 x decibel; Defaults: K1[0] 0 K1[1] -60000 K1[2] -60000 K1[3] -60000 K1[4] 0 K1[5] 0 K2[0] 0 K2[1] -11200 K2[2] -7419 K2[3] -7419 K2[4] 0 K2[5] 0)

  The PSD values specified are in units of 1000 x decibel (dB). For example, 60000 means 60.0 dB. The actual power levels implemented are in milliwatts per Hertz (dBm/Hz). For example, you would enter -60000 with this command to specify a value of -60 dBm/Hz.

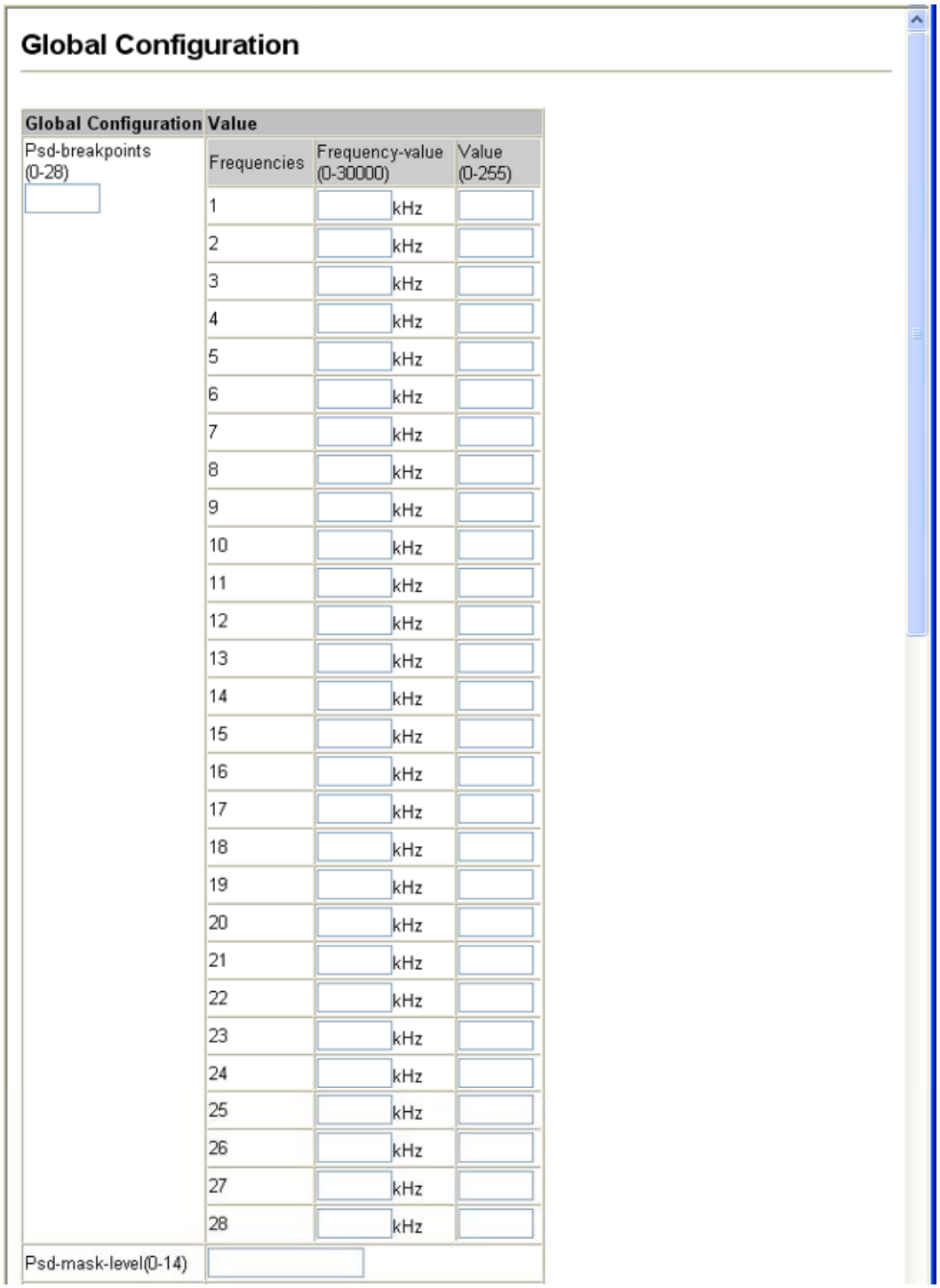
Downloaded from www.Manualslib.com manuals search engine

Upstream power back-off (UPBO) is used to mitigate far-end crosstalk caused by upstream transmissions from shorter to longer loops. The bounding power levels specified in this table are used to reshape the PSD, ensuring that the signals on short to long loops are compatible. The transceiver will adjust its transmitted signal to conform to the power limitations set in this table.

If upstream power backoff is enabled, the transceiver will automatically reduce the PSD at each frequency breakpoint set the by the PSD breakpoint specified on the Global Configuration screen or the VDSL Port Configuration screen (see page 10-7).

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, Global Configuration. Configure the required items, and click Apply. (Note that the parameters in the following screen are all set to their default values.)



Downloaded from www.Manualslib.com manuals search engine

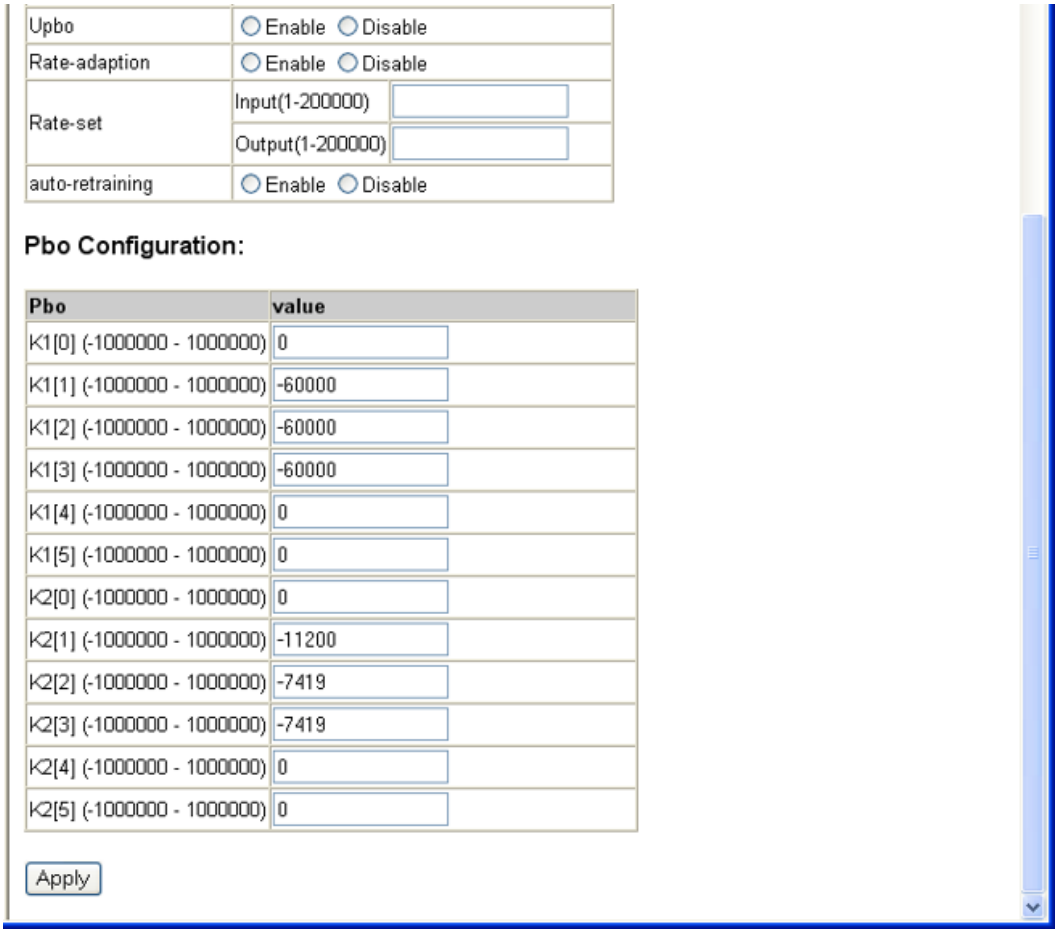


Figure 10-1 VDSL Global Configuration

CLI – This example displays sample settings for some of the VDSL global configuration commands.

```
Console(config)#lre psd-breakpoint 5                              29-12
Console(config)#lre psd-frequencies 1 3750                        29-13
Console(config)#lre psd-value 1 240                               29-15
Console(config)#lre psd-mask-level 5                              29-16
Console(config)#lre upbo                                          29-19
Console(config)#lre rate-adaption                                 29-33
Console(config)#lre rate-set input 200000                         29-27
Console(config)#lre auto-retraining                               29-31
Console(config)#lre pbo-config k1[0] 0 k1[1] -60000 k1[2] -60000
  k1[3] -60000 k1[4] 0  k1[5] 0 k2[0] 0 k2[1] -11200 k2[2] -7419
  k2[3] -7419 k2[4] 0 k2[5] 0
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Interface Settings for VDSL Ports

This section describes how to configure communication parameters for VDSL ports such as specifying data band usage plans, setting notches within the frequency bands to avoid interference with ham radio signals, setting a mask for power spectral density to meet regional or local limitations for transmitting signals on phone lines, setting an acceptable target for the signal-to-noise ratio, and enabling automatic rate adaptation.

Command Attributes

Buttons in Upper Menu Bar

- **Interface Port** – Port identifier. (Range: 1-16)
- **Retraining** – Manually initiates rate adaptation to find the optimal transmission rate based on existing line conditions.

  Manual retraining can be used if auto-retraining has been disabled on the VDSL Global Configuration screen (page 10-6), and the signal quality or link on a port has dropped. Retraining initiates rate adaptation and selects the optimal transmission rate based on existing line conditions and the bounds set in the Data Rate field.

  Note that it might take several minutes to retrain a port.
- **Shut Down** – Shuts down a VDSL port.

  This command can be used to disable the VDSL chipset transmitter of a port that is not connected to a working CPE. In some unusual circumstances, the power emitted by VDSL ports can affect other VDSL ports. It is recommended that ports that are not wired to CPEs be shut down in this way. This command can also be used to disable access to the switch from this port for troubleshooting or security reasons.
- **Start Up** – Re-enabled a port that has been previously shut down.
- **Reset** – Resets the VDSL controller chip for the specified VDSL port

  A port may need to be reset in order to troubleshoot VDSL connection or performance problems.

Downloaded from www.Manualslib.com manuals search engine

Configuration Tables

- **Channel Mode** – Sets the channel mode to fast or interleaved. (Default: Interleaved)

  Interleaving protects data against bursts of errors by using the Reed-Solomon error correction algorithm to spread the errors over a number of code words. A greater degree of interleaving provides more protection against noise pulses, but increases transmission delay and reduces the effective bandwidth.

  For applications that cannot tolerate latency (for example, voice), use the fast mode to disable the interleaving burst error correction method.

- **Interleave Max Delay** – Sets the maximum interleave delay. (Range: 0-40, in units of 0.5 ms; Default: 4x0.5 ms or 2 ms)

  Interleaving causes a delay in the transmission of data.

  Setting the interleave delay to a value of zero disables interleaving.

  Interleave delay applies only to the interleave (slow) channel and defines the mapping (relative spacing) between subsequent input bytes at the interleaver input and their placement in the bit stream at the interleaver output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream allowing for improved impulse noise immunity at the expense of payload latency.

- **Ham Band** – Sets the Handheld Amateur Radio (HAM) band that will be blocked to VDSL signals based on defined frequencies. (Options: See Table 29-4, "HAM Band Notches," on page 29-7. Default: none)

  Using a HAM band mask prevents interference with other systems (e.g., amateur radio) that use narrow band transmission in the VDSL frequency band. The selected frequency range will not be used to transmit data on the VDSL line. You may need to specify a mask for a specific radio frequency range if required by local regulations or if specific incidents of interference are reported within a service area.

  Note that the RFI-Band field includes information on both the frequency range and the corresponding standard.

Downloaded from www.Manualslib.com manuals search engine

- **Region Ham Band** – Sets the ham radio band that will be blocked to VDSL signals based on defined usage types. (Options: See Table 29-5, "HAM Band Notches for Usage Types," on page 29-10. Default: none)

  Using a HAM band mask prevents interference with other systems (e.g., amateur radio) that use narrow band transmission in the VDSL frequency band. The selected frequency range will not be used to transmit data on the VDSL line. You may need to specify a mask for a specific radio signal usage type if required by local regulations or if specific incidents of interference are reported within a service area.

  Abbreviation used in the RFI-Band field include the following items:

  GMDSS: Global Maritime Distress and Safety System
  DRM: Digital Radio Mondiale (Digital Radio Broadcasting)
  CB: Citizen's Band Radio

- **Band Plan** – Sets the frequency bands used for VDSL signals based on a set of predefined plans. (Options: See Table 29-3, "VDSL2 Band Plans," on page 29-5. Default: 998-640-30000 100/100)

  The band plan options are described by ITU-T Standards G.9932. The first field in the band plan designator indicates the ITU standard, the second field indicates the lower frequency bound, and the third field indicates the upper frequency bound.

- **Option Band** – Sets the frequencies to be used for the optional Upstream Band 0 (US0). Note that each option includes a range for the low and high end frequencies.

  Options: No optional band (default)
  ITU-T G993.2, Annex A, 6-32 kHz, 26-138 kHz
  ITU-T G993.2, Annex B, 32-64 kHz, 138-276 kHz
  ITU-T G993.2, Annex B, 6-64 kHz, 26-276 kHz

  Performance enhancements have been incorporated in G.993.2 for the optional US0 band (specifically, support in initialization for training of time domain equalizers and echo cancellers) which provide reliable operation on loops up to approximately 2500 meters of 26 AWG (0.4 mm).

Downloaded from www.Manualslib.com manuals search engine

- **PSD Breakpoints** –
  See "Configuring Global Settings for VDSL Ports" on page 10-1.
- **PSD Mask Level** –
  See "Configuring Global Settings for VDSL Ports" on page 10-1.
- **UPBO** –
  See "Configuring Global Settings for VDSL Ports" on page 10-1.
- **Tone** – Disables downstream or upstream VDSL signals at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz. (Default: Disable tones at 640 KHz and below)

  This parameter specifies a frequency beneath which VDSL signals are not allowed. For example, the default lower frequency bound for DS1 defined in Annex C of G.993.2 is 640 KHz. The low-end frequencies filtered out by this parameter are used for common POTS or ISDN services.

  The frequency bound specified by this parameter takes precedence over that defined in the selected band plan.
- **Data Rate** – Specifies the minimum and maximum data rate for downstream and upstream fast or slow (interleaved) channels. (Default: 64 kbps minimum, 200,000 kbps maximum)

  The parameter sets the minimum and maximum data rates supported by each upstream and downstream band. Bounding data rates should be set for both fast and slow channels if operation may sometimes disable or enable interleaving. These bounds are applied to the specified interface when rate adaption is enabled.
- **Max Power** – Sets the maximum aggregate downstream or upstream power. (Range: 0-255, in units of 0.25 dBm; Default:255, which is equivalent to 63.75 dBm)
- **Min Protection** – Configures the minimum level of impulse noise protection for all bearer channels. This is expressed in the number of consecutive DMT symbols for which errors can be completely corrected. (Range: 0-255, in units of 0.5 DMT symbols, or 125 microseconds; Default: 0)

Downloaded from www.Manualslib.com manuals search engine

This minimum margin indicates the amount of increase in impulse noise that the system can tolerate under operational conditions while still ensuring required transmission quality.

This parameter is used to set the time span of impulse noise protection, as seen at the input to the de-interleaver, for which errors can be completely corrected by the error correcting code, regardless of the number of errors within the errored DMT symbols.

Note that this parameter only applies to interleaved channels. Refer to ITU-T G.993.2 for a full description of the methods used to calculate the minimum level of impulse noise protection.

- **Noise Margin** – The signal-to-noise margin.
  - **Target** – Configures the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization. (Range: 0-62, in units of 0.5 dB; Default: 12 dB)

    This parameter sets the noise margin that transceivers must achieve with a Bit Error Rate (BER) of 10^{-7} or better to successfully complete initialization. It indicates the maximum amount by which the reference crosstalk noise level can be increased during a BER test without causing the modem to fail the BER requirement.
  - **Minimum** – Configures the minimum acceptable signal-to-noise margin. (Range: 0-62, in units of 0.5 dB; Default: 10 dB)

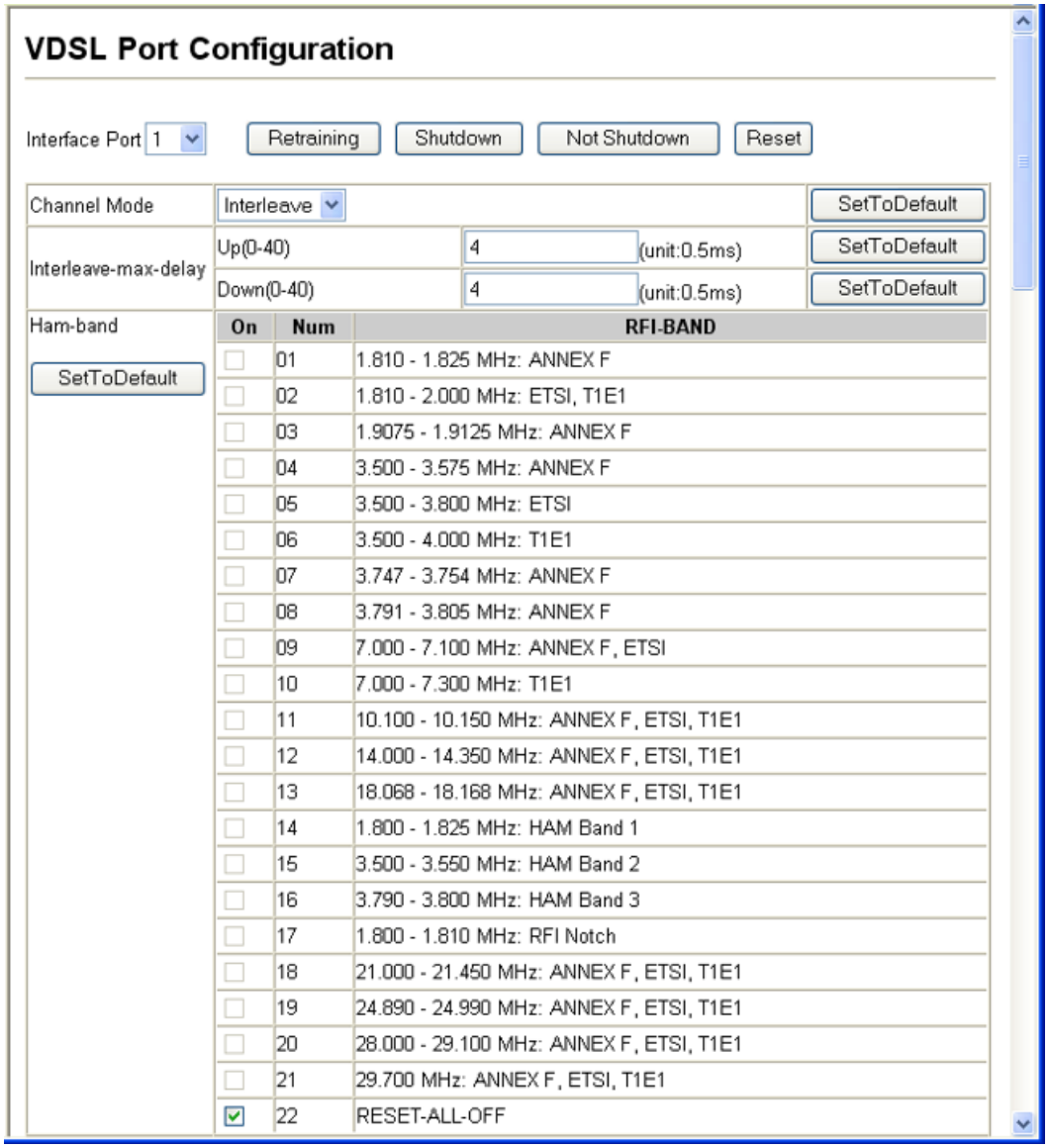
    This parameter sets the minimum noise margin the receiver can tolerate. If the noise margin falls below this level, the receiver will ask the sender to increase its transmit power. If it is not possible to increase the transmit power, a loss-of-margin defect occurs, the link will fail and the receiver will attempt to re-initialize.

    When rate adaptation is enabled, the signal-to-noise ratio (SNR) is an indicator of link quality. The switch itself has no internal functions to ensure link quality. To ensure a stable link, you should add a margin to the theoretical minimum signal-to-noise ratio (SNR).
- **Rate Adaption** –

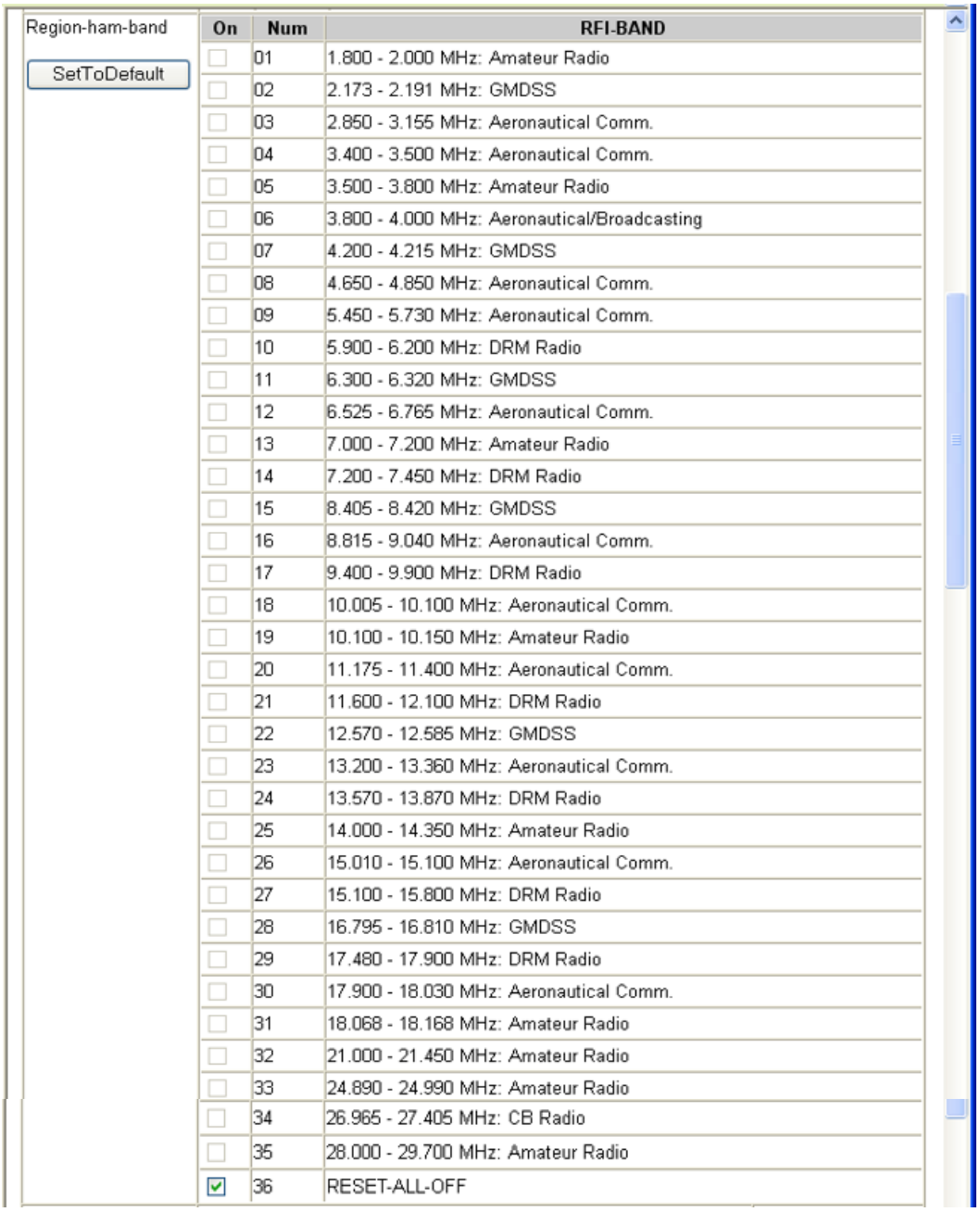
  See "Configuring Global Settings for VDSL Ports" on page 10-1.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, VDSL Port Configuration. Select one of the VDSL ports from the scroll-down list, set the required parameters, and click Apply. (Note that the parameters in the following screen are all set to their default values.)


VDSL Port Configuration
Interface Port 1
Retraining
Shutdown
Not Shutdown
Reset
Channel Mode
Interleave
SetToDefault
Interleave-max-delay
Up(0-40)
4
(unit:0.5ms)
SetToDefault
Down(0-40)
4
(unit:0.5ms)
SetToDefault
Ham-band
SetToDefault
On
Num
RFI-BAND
01 1.810 - 1.825 MHz: ANNEX F
02 1.810 - 2.000 MHz: ETSI, T1E1
03 1.9075 - 1.9125 MHz: ANNEX F
04 3.500 - 3.575 MHz: ANNEX F
05 3.500 - 3.800 MHz: ETSI
06 3.500 - 4.000 MHz: T1E1
07 3.747 - 3.754 MHz: ANNEX F
08 3.791 - 3.805 MHz: ANNEX F
09 7.000 - 7.100 MHz: ANNEX F, ETSI
10 7.000 - 7.300 MHz: T1E1
11 10.100 - 10.150 MHz: ANNEX F, ETSI, T1E1
12 14.000 - 14.350 MHz: ANNEX F, ETSI, T1E1
13 18.068 - 18.168 MHz: ANNEX F, ETSI, T1E1
14 1.800 - 1.825 MHz: HAM Band 1
15 3.500 - 3.550 MHz: HAM Band 2
16 3.790 - 3.800 MHz: HAM Band 3
17 1.800 - 1.810 MHz: RFI Notch
18 21.000 - 21.450 MHz: ANNEX F, ETSI, T1E1
19 24.890 - 24.990 MHz: ANNEX F, ETSI, T1E1
20 28.000 - 29.100 MHz: ANNEX F, ETSI, T1E1
21 29.700 MHz: ANNEX F, ETSI, T1E1
22 RESET-ALL-OFF

Downloaded from www.Manualslib.com manuals search engine

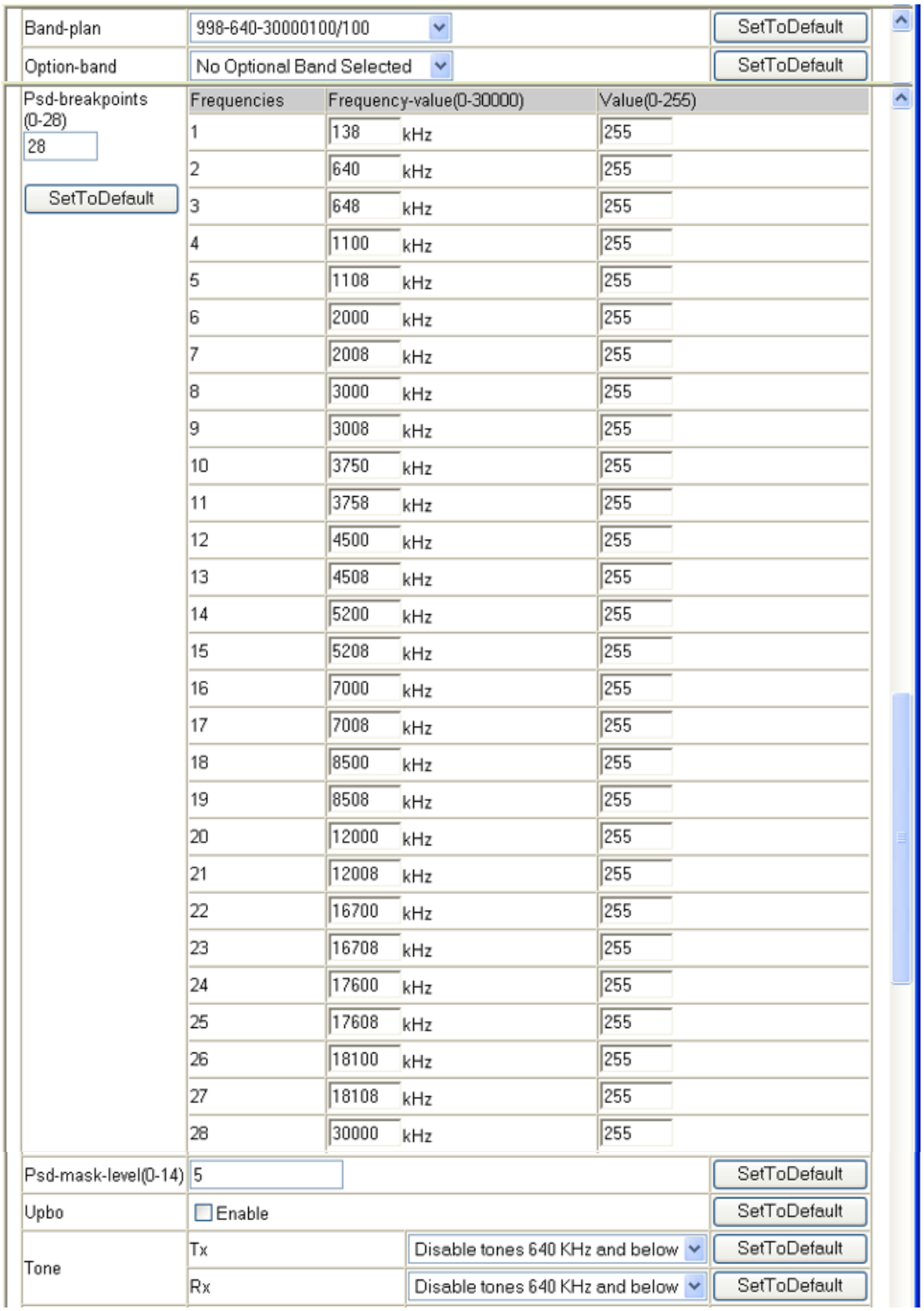


Region-ham-band

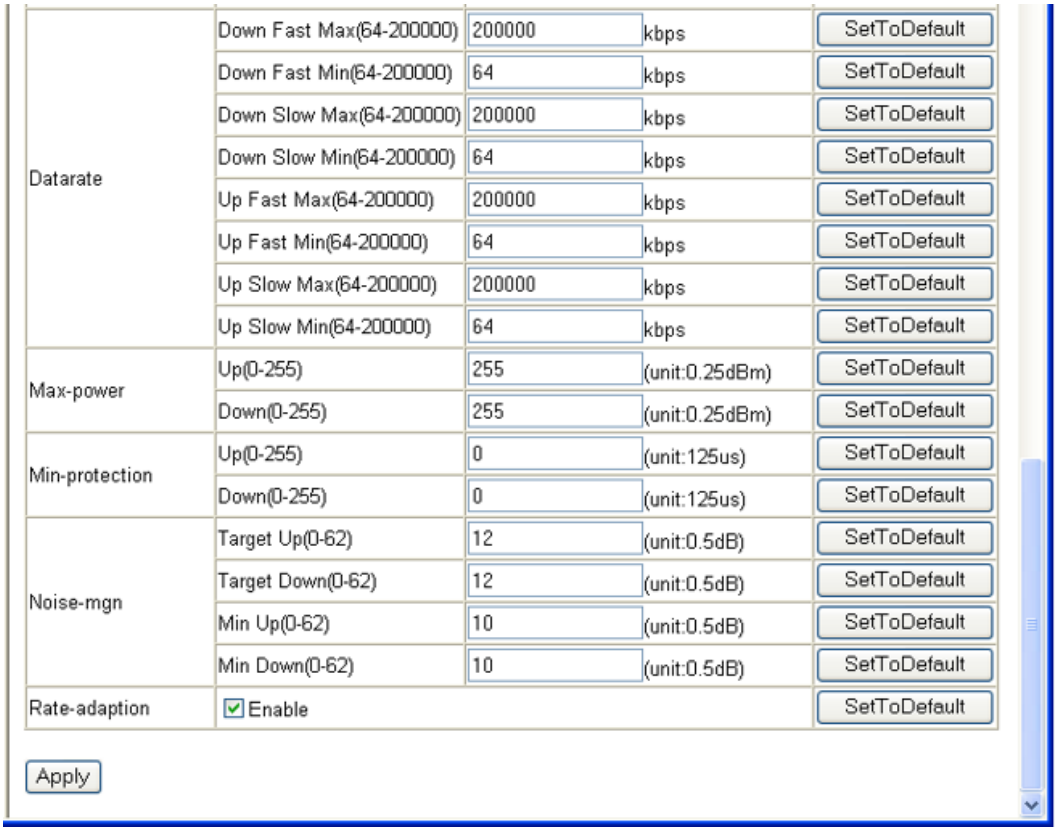
SetToDefault

On	Num	RFI-BAND
☐	01	1.800 - 2.000 MHz: Amateur Radio
☐	02	2.173 - 2.191 MHz: GMDSS
☐	03	2.850 - 3.155 MHz: Aeronautical Comm.
☐	04	3.400 - 3.500 MHz: Aeronautical Comm.
☐	05	3.500 - 3.800 MHz: Amateur Radio
☐	06	3.800 - 4.000 MHz: Aeronautical/Broadcasting
☐	07	4.200 - 4.215 MHz: GMDSS
☐	08	4.650 - 4.850 MHz: Aeronautical Comm.
☐	09	5.450 - 5.730 MHz: Aeronautical Comm.
☐	10	5.900 - 6.200 MHz: DRM Radio
☐	11	6.300 - 6.320 MHz: GMDSS
☐	12	6.525 - 6.765 MHz: Aeronautical Comm.
☐	13	7.000 - 7.200 MHz: Amateur Radio
☐	14	7.200 - 7.450 MHz: DRM Radio
☐	15	8.405 - 8.420 MHz: GMDSS
☐	16	8.815 - 9.040 MHz: Aeronautical Comm.
☐	17	9.400 - 9.900 MHz: DRM Radio
☐	18	10.005 - 10.100 MHz: Aeronautical Comm.
☐	19	10.100 - 10.150 MHz: Amateur Radio
☐	20	11.175 - 11.400 MHz: Aeronautical Comm.
☐	21	11.600 - 12.100 MHz: DRM Radio
☐	22	12.570 - 12.585 MHz: GMDSS
☐	23	13.200 - 13.360 MHz: Aeronautical Comm.
☐	24	13.570 - 13.870 MHz: DRM Radio
☐	25	14.000 - 14.350 MHz: Amateur Radio
☐	26	15.010 - 15.100 MHz: Aeronautical Comm.
☐	27	15.100 - 15.800 MHz: DRM Radio
☐	28	16.795 - 16.810 MHz: GMDSS
☐	29	17.480 - 17.900 MHz: DRM Radio
☐	30	17.900 - 18.030 MHz: Aeronautical Comm.
☐	31	18.068 - 18.168 MHz: Amateur Radio
☐	32	21.000 - 21.450 MHz: Amateur Radio
☐	33	24.890 - 24.990 MHz: Amateur Radio
☐	34	26.965 - 27.405 MHz: CB Radio
☐	35	28.000 - 29.700 MHz: Amateur Radio
☑	36	RESET-ALL-OFF

Downloaded from www.Manualslib.com manuals search engine



Downloaded from www.Manualslib.com manuals search engine



Datarate	Down Fast Max(64-200000)	200000	kbps	SetToDefault
	Down Fast Min(64-200000)	64	kbps	SetToDefault
	Down Slow Max(64-200000)	200000	kbps	SetToDefault
	Down Slow Min(64-200000)	64	kbps	SetToDefault
	Up Fast Max(64-200000)	200000	kbps	SetToDefault
	Up Fast Min(64-200000)	64	kbps	SetToDefault
	Up Slow Max(64-200000)	200000	kbps	SetToDefault
	Up Slow Min(64-200000)	64	kbps	SetToDefault
Max-power	Up(0-255)	255	(unit:0.25dBm)	SetToDefault
	Down(0-255)	255	(unit:0.25dBm)	SetToDefault
Min-protection	Up(0-255)	0	(unit:125us)	SetToDefault
	Down(0-255)	0	(unit:125us)	SetToDefault
Noise-mgn	Target Up(0-62)	12	(unit:0.5dB)	SetToDefault
	Target Down(0-62)	12	(unit:0.5dB)	SetToDefault
	Min Up(0-62)	10	(unit:0.5dB)	SetToDefault
	Min Down(0-62)	10	(unit:0.5dB)	SetToDefault
Rate-adaption	Enable			SetToDefault

Apply

Figure 10-2 VDSL Port Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This example displays sample settings for some of the VDSL port configuration commands.

```
Console(config)#interface ethernet 1/1                          25-13
Console(config-if)#lre reset remote                             29-30
Console(config-if)#lre retraining                               29-32
Console(config-if)#lre channel interleave                       29-24
Console(config-if)#lre interleave-max-delay down 6              29-25
Console(config-if)#lre ham-band 11                              29-7
Console(config-if)#lre region-ham-band 34                       29-9
Console(config-if)#lre band-plan 5                              29-4
Console(config-if)#lre option-band 2                            29-6
Console(config-if)#lre psd-breakpoint 5                         29-12
Console(config-if)#lre psd-frequencies 1 3750                   29-13
Console(config-if)#lre psd-value 1 240                          29-15
Console(config-if)#lre psd-mask-level 5                         29-16
Console(config-if)#lre upbo                                     29-19
Console(config-if)#lre tone tx 2                                29-21
Console(config-if)#lre datarate down fast max 190000            29-26
Console(config-if)#lre max-power down 58                        29-22
Console(config-if)#lr min-protection down 5                     29-23
Console(config-if)#lre noise-mgn target down 30                 29-28
Console(config-if)#lre noise-mgn min down 28                    29-29
Console(config-if)#lre lre rate-adaption                        29-33
Console(config-if)#
```

Configuring Line Profiles

This section describes how to configure a list of communication parameters such as data rates and acceptable noise margins which can be applied to all VDSL ports or to a selected group of ports.

Command Attributes

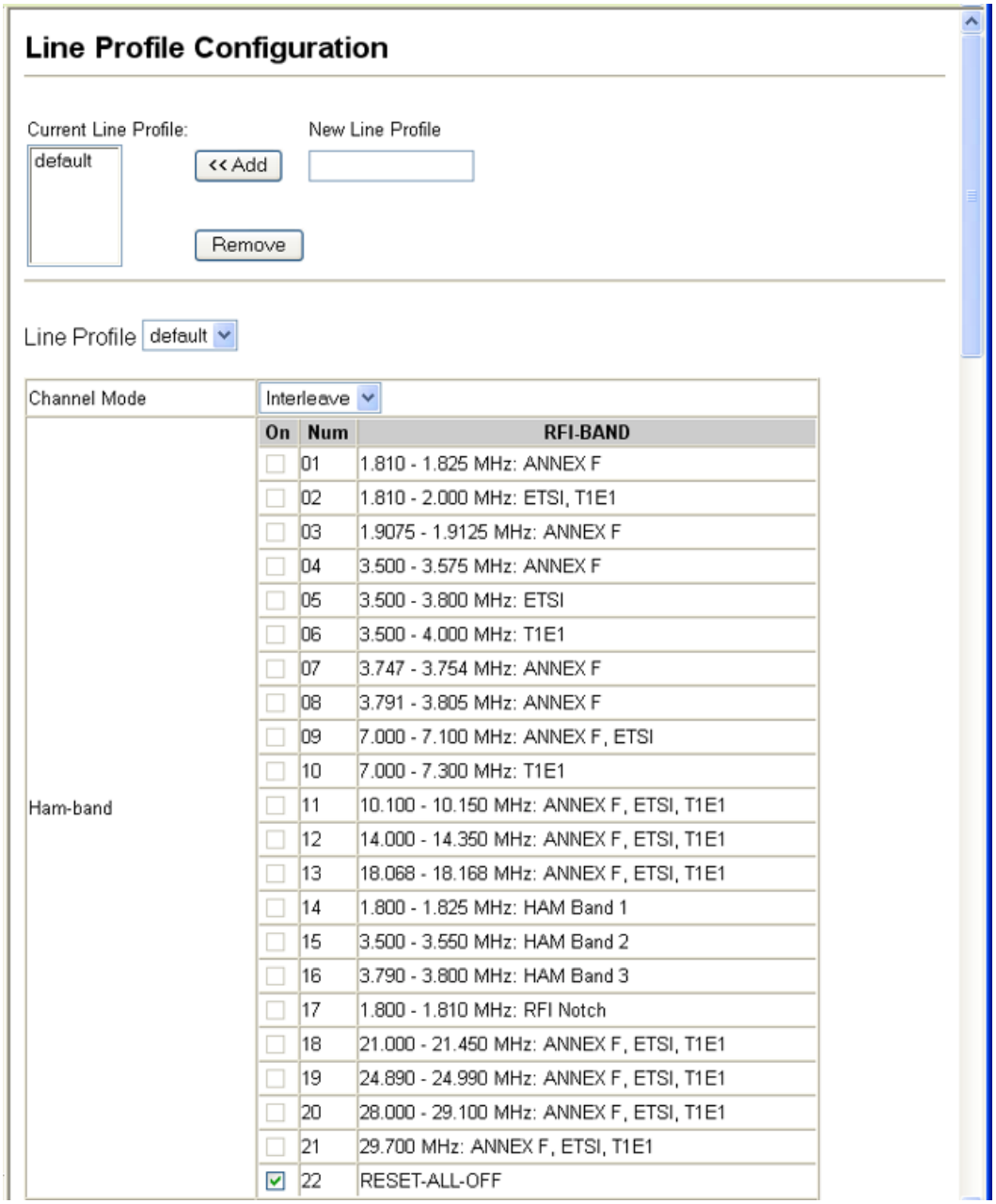
- **Line Profile** – Name of the profile. (Range: 1-31 alphanumeric characters)

  The default profile includes the system default settings for VDSL lines.
- **Up/Down Max Interleave Delay** – See Interleave Max Delay under "Configuring Interface Settings for VDSL Ports" on page 10-7.
- **Line Profile Mapping** – Applies a line profile to selected VDSL ports.

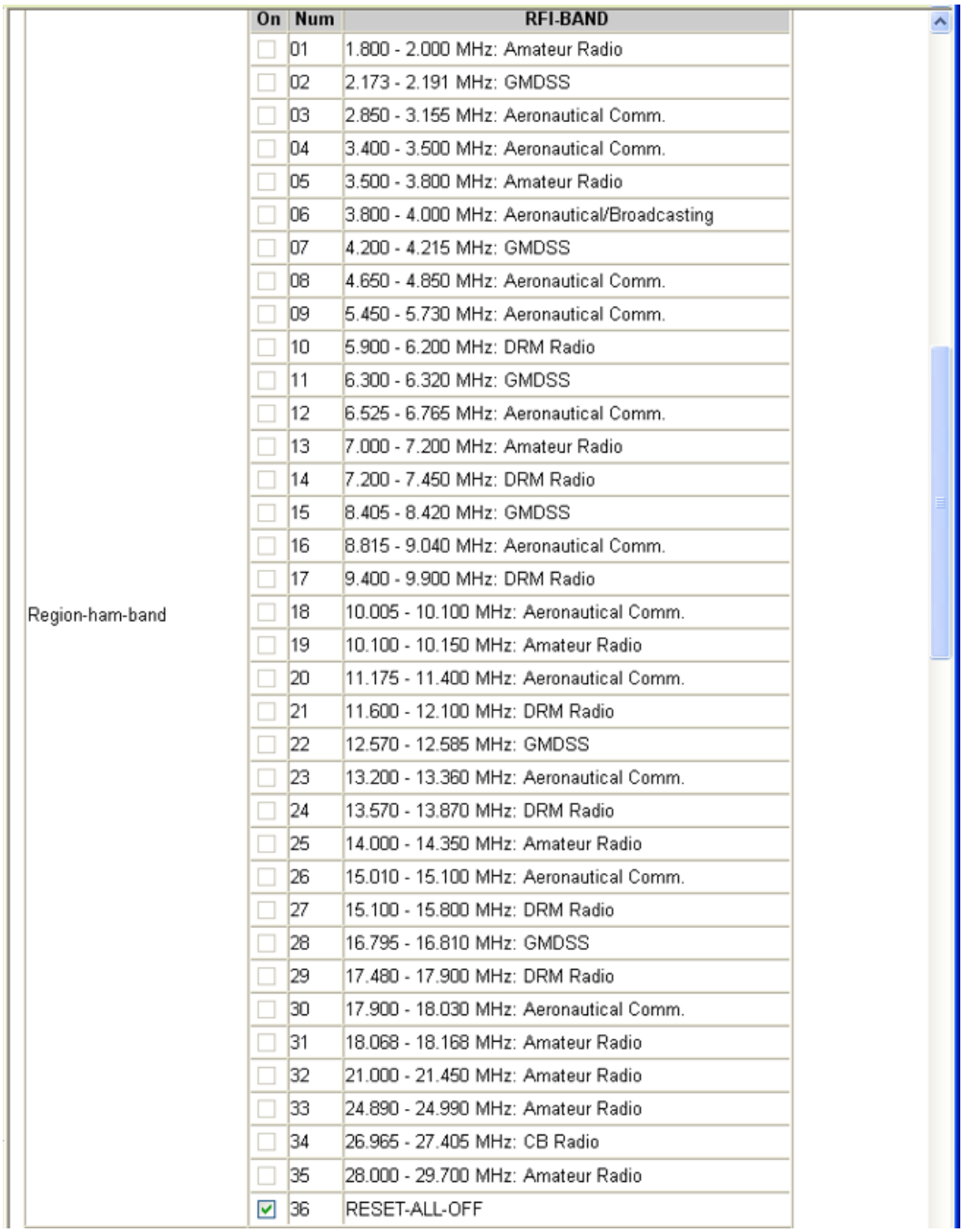
For a description of the other parameters listed in the Line Profile table, see "Configuring Interface Settings for VDSL Ports" on page 10-7.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, Line Profile Configuration. Select a line profile from the drop-down list above the Line Profile table of connection parameters, configure the required items in this table, and then click the Apply button beneath the table to store the profile settings. Now select the required line profile from the drop-down list in the Line Profile Mapping table, and click the Apply button next to the VDSL ports to apply the selected profile.

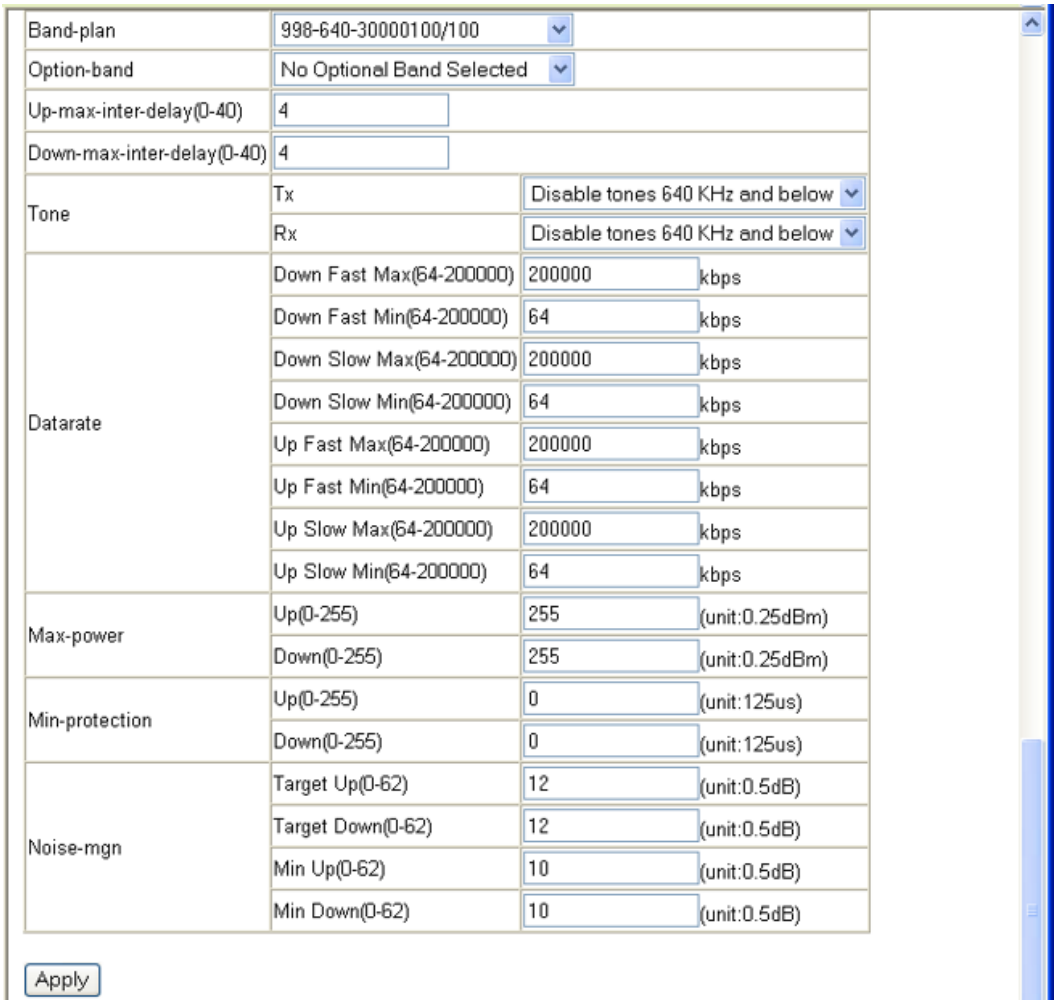

Line Profile Configuration
Current Line Profile:
default
<< Add
Remove
New Line Profile
Line Profile default
Channel Mode
Interleave
Ham-band
On
Num
RFI-BAND
01 1.810 - 1.825 MHz: ANNEX F
02 1.810 - 2.000 MHz: ETSI, T1E1
03 1.9075 - 1.9125 MHz: ANNEX F
04 3.500 - 3.575 MHz: ANNEX F
05 3.500 - 3.800 MHz: ETSI
06 3.500 - 4.000 MHz: T1E1
07 3.747 - 3.754 MHz: ANNEX F
08 3.791 - 3.805 MHz: ANNEX F
09 7.000 - 7.100 MHz: ANNEX F, ETSI
10 7.000 - 7.300 MHz: T1E1
11 10.100 - 10.150 MHz: ANNEX F, ETSI, T1E1
12 14.000 - 14.350 MHz: ANNEX F, ETSI, T1E1
13 18.068 - 18.168 MHz: ANNEX F, ETSI, T1E1
14 1.800 - 1.825 MHz: HAM Band 1
15 3.500 - 3.550 MHz: HAM Band 2
16 3.790 - 3.800 MHz: HAM Band 3
17 1.800 - 1.810 MHz: RFI Notch
18 21.000 - 21.450 MHz: ANNEX F, ETSI, T1E1
19 24.890 - 24.990 MHz: ANNEX F, ETSI, T1E1
20 28.000 - 29.100 MHz: ANNEX F, ETSI, T1E1
21 29.700 MHz: ANNEX F, ETSI, T1E1
22 RESET-ALL-OFF

Downloaded from www.Manualslib.com manuals search engine



	On	Num	RFI-BAND
Region-ham-band	☐	01	1.800 - 2.000 MHz: Amateur Radio
	☐	02	2.173 - 2.191 MHz: GMDSS
	☐	03	2.850 - 3.155 MHz: Aeronautical Comm.
	☐	04	3.400 - 3.500 MHz: Aeronautical Comm.
	☐	05	3.500 - 3.800 MHz: Amateur Radio
	☐	06	3.800 - 4.000 MHz: Aeronautical/Broadcasting
	☐	07	4.200 - 4.215 MHz: GMDSS
	☐	08	4.650 - 4.850 MHz: Aeronautical Comm.
	☐	09	5.450 - 5.730 MHz: Aeronautical Comm.
	☐	10	5.900 - 6.200 MHz: DRM Radio
	☐	11	6.300 - 6.320 MHz: GMDSS
	☐	12	6.525 - 6.765 MHz: Aeronautical Comm.
	☐	13	7.000 - 7.200 MHz: Amateur Radio
	☐	14	7.200 - 7.450 MHz: DRM Radio
	☐	15	8.405 - 8.420 MHz: GMDSS
	☐	16	8.815 - 9.040 MHz: Aeronautical Comm.
	☐	17	9.400 - 9.900 MHz: DRM Radio
	☐	18	10.005 - 10.100 MHz: Aeronautical Comm.
	☐	19	10.100 - 10.150 MHz: Amateur Radio
	☐	20	11.175 - 11.400 MHz: Aeronautical Comm.
	☐	21	11.600 - 12.100 MHz: DRM Radio
	☐	22	12.570 - 12.585 MHz: GMDSS
	☐	23	13.200 - 13.360 MHz: Aeronautical Comm.
	☐	24	13.570 - 13.870 MHz: DRM Radio
	☐	25	14.000 - 14.350 MHz: Amateur Radio
	☐	26	15.010 - 15.100 MHz: Aeronautical Comm.
	☐	27	15.100 - 15.800 MHz: DRM Radio
	☐	28	16.795 - 16.810 MHz: GMDSS
	☐	29	17.480 - 17.900 MHz: DRM Radio
	☐	30	17.900 - 18.030 MHz: Aeronautical Comm.
	☐	31	18.068 - 18.168 MHz: Amateur Radio
	☐	32	21.000 - 21.450 MHz: Amateur Radio
	☐	33	24.890 - 24.990 MHz: Amateur Radio
	☐	34	26.965 - 27.405 MHz: CB Radio
	☐	35	28.000 - 29.700 MHz: Amateur Radio
	☑	36	RESET-ALL-OFF

Downloaded from www.Manualslib.com manuals search engine



Band-plan	998-640-30000100/100		
Option-band	No Optional Band Selected		
Up-max-inter-delay(0-40)	4		
Down-max-inter-delay(0-40)	4		
Tone	Tx	Disable tones 640 KHz and below	
	Rx	Disable tones 640 KHz and below	
Datarate	Down Fast Max(64-200000)	200000	kbps
	Down Fast Min(64-200000)	64	kbps
	Down Slow Max(64-200000)	200000	kbps
	Down Slow Min(64-200000)	64	kbps
	Up Fast Max(64-200000)	200000	kbps
	Up Fast Min(64-200000)	64	kbps
	Up Slow Max(64-200000)	200000	kbps
	Up Slow Min(64-200000)	64	kbps
Max-power	Up(0-255)	255	(unit:0.25dBm)
	Down(0-255)	255	(unit:0.25dBm)
Min-protection	Up(0-255)	0	(unit:125us)
	Down(0-255)	0	(unit:125us)
Noise-mgn	Target Up(0-62)	12	(unit:0.5dB)
	Target Down(0-62)	12	(unit:0.5dB)
	Min Up(0-62)	10	(unit:0.5dB)
	Min Down(0-62)	10	(unit:0.5dB)

Apply

Downloaded from www.Manualslib.com manuals search engine

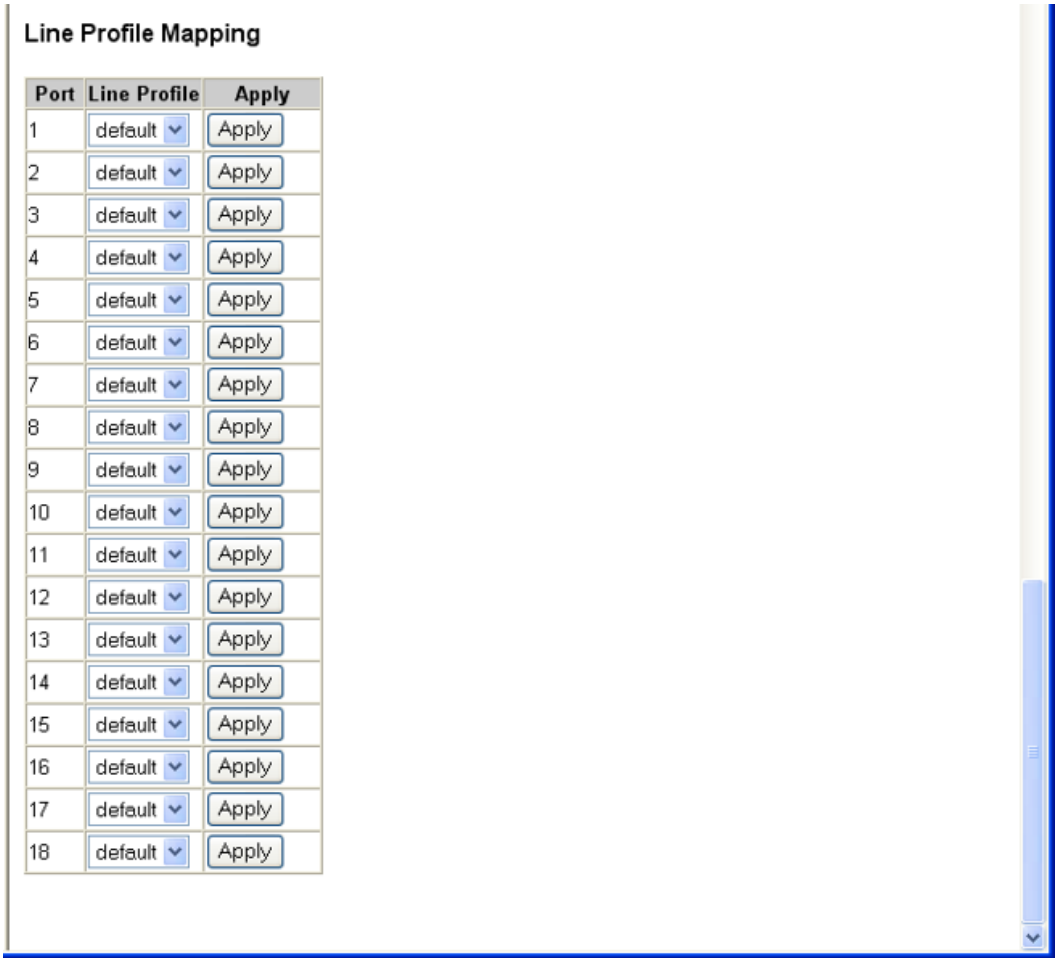


Figure 10-3 Line Profile Configuration

CLI – This example displays sample settings for a line profile.

```
Console(config)#line-profile southport                          29-36
Console(config-line-profile)#channel interleave                 29-45
Console(config-line-profile)#ham-band 11                        29-40
Console(config-line-profile)#region-ham-band 34                 29-41
Console(config-line-profile)#band-plan 5                        29-38
Console(config-line-profile)#option-band 2                      29-39
Console(config-line-profile)#down-max-inter-delay 6             29-46
Console(config-line-profile)#tone tx 2                          29-42
Console(config-line-profile)#down-fast-max-datarate 190000      29-47
Console(config-line-profile)#max-power down 58                  29-43
Console(config-line-profile)#min-protection down 5              29-44
Console(config-line-profile)#down-target-noise-mgn 12           29-48
Console(config-line-profile)#down-min-noise-mgn 12              29-49
Console(config-line-profile)#exit
Console(config)#interface ethernet 1/1                          25-13
Console(config-if)#lre line-profile southport                   29-37
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying VDSL Status Information

This section describes the information displayed for VDSL configuration settings, signal status, and communication statistics.

Field Attributes

LRE Status – Communication status of the VDSL line

Table 10-1 LRE Status

Parameter	Description
Port Status	The current initialization or operational status.
Training Margin	The targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization (see Noise Margin in "Configuring Interface Settings for VDSL Ports" on page 10-7).
Line Protection (Slow Path)	The minimum level of impulse noise protection for all bearer channels (see Min Protection in "Configuring Interface Settings for VDSL Ports" on page 10-7).
Downstream/ Upstream Delay	The maximum interleave delay (see Interleave Max Delay in "Configuring Interface Settings for VDSL Ports" on page 10-7).
Tx Total Power	The maximum aggregate transmit power over all signal bands for the specified interface.
FE Tx Total Power	The maximum transmit power used at the far end.
VDSL Estimated Loop Length	Estimated length of the VDSL connection; used to calculate power backoff.
G.Hs Estimated Loop Length	Estimated length of the VDSL connection; used for handshaking.
Current Framing Mode	Only Packet Transfer Mode (PTM) framing is used for VDSL lines.
Far End Capabilities Mask	The capabilities supported by the attached CPE.
SNR Margin	Current signal-to-noise margin
Attenuation	Amount of attenuation in signal strength

Downloaded from www.Manualslib.com manuals search engine

Table 10-1 LRE Status (Continued)

Parameter	Description
Avg SNR Margin	Average signal-to-noise margin above the SNR.
Avg SNR	Average signal-to-noise ratio.

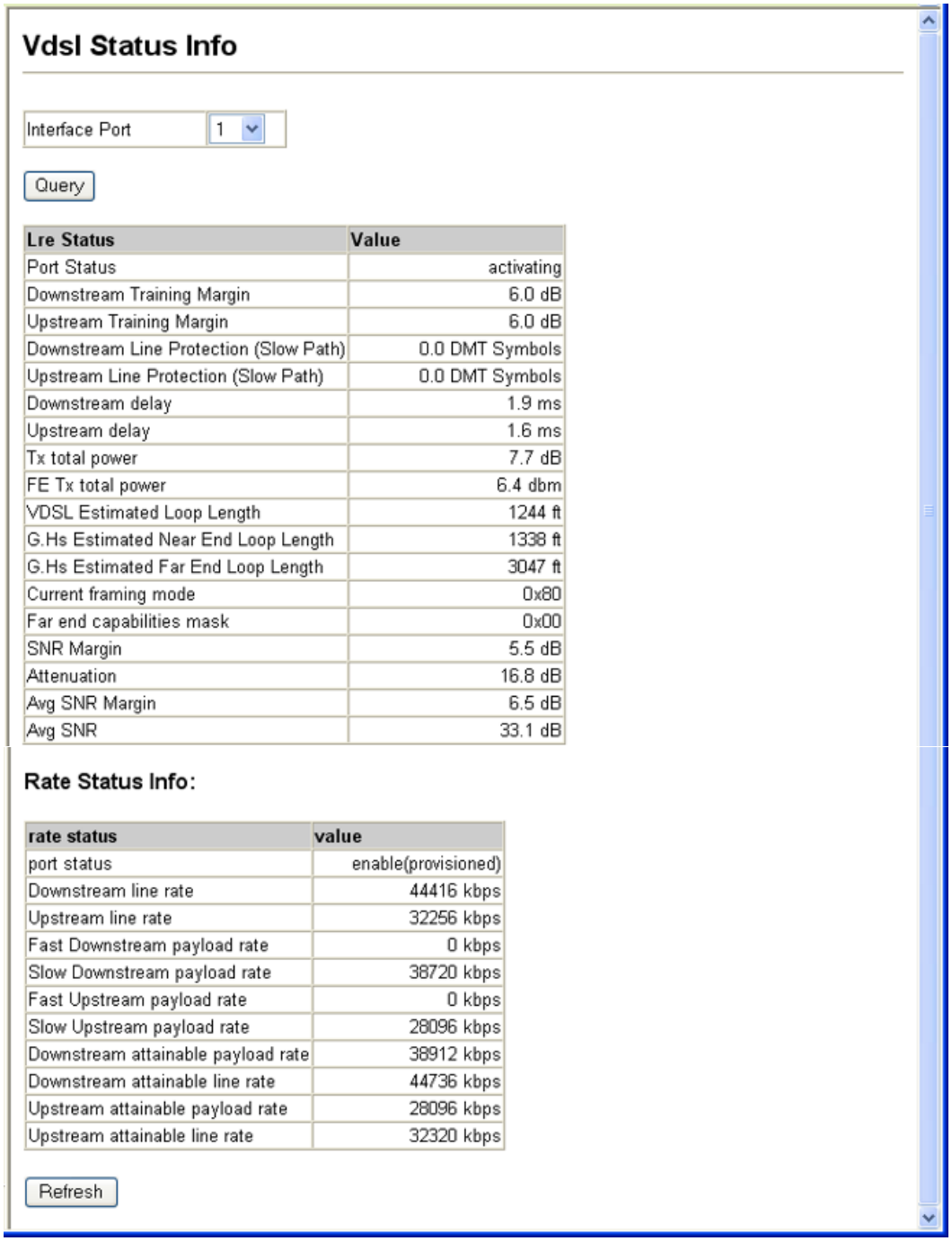
LRE Rate Information – Data Rates for the VDSL line

Table 10-2 Rate Status

Parameter	Description
Port Status	Indicates if the port is administratively enabled or disabled.
Line Rate	The downstream and upsteam line rate.
Payload Rate	The actual payload carried on the fast and interleaved channels.
Attainable Payload Rate	The maximum attainable payload on the downstream and upstream channels.
Attainable Line Rate	The maximum attainable line rate on the downstream and upstream channels

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, VDSL Status Information. Select a VDSL port from the drop-down list, and click Query.



Vdsl Status Info

Interface Port 1

Query

Lre Status	Value
Port Status	activating
Downstream Training Margin	6.0 dB
Upstream Training Margin	6.0 dB
Downstream Line Protection (Slow Path)	0.0 DMT Symbols
Upstream Line Protection (Slow Path)	0.0 DMT Symbols
Downstream delay	1.9 ms
Upstream delay	1.6 ms
Tx total power	7.7 dB
FE Tx total power	6.4 dbm
VDSL Estimated Loop Length	1244 ft
G.Hs Estimated Near End Loop Length	1338 ft
G.Hs Estimated Far End Loop Length	3047 ft
Current framing mode	0x80
Far end capabilities mask	0x00
SNR Margin	5.5 dB
Attenuation	16.8 dB
Avg SNR Margin	6.5 dB
Avg SNR	33.1 dB

Rate Status Info:

rate status	value
port status	enable(provisioned)
Downstream line rate	44416 kbps
Upstream line rate	32256 kbps
Fast Downstream payload rate	0 kbps
Slow Downstream payload rate	38720 kbps
Fast Upstream payload rate	0 kbps
Slow Upstream payload rate	28096 kbps
Downstream attainable payload rate	38912 kbps
Downstream attainable line rate	44736 kbps
Upstream attainable payload rate	28096 kbps
Upstream attainable line rate	32320 kbps

Refresh

Figure 10-4 VDSL Status Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This example displays connection status and data rates for the selected VDSL port.

```
Console#show lre 1/1                                                    29-79
port 1 status :                              port enable(provisioned)
port 1 status :                              port activating
Downstream Training Margin:                  8.0 dB
Upstream Training Margin:                    9.1 dB
Downstream Line Protection (Slow Path):      0.0 DMT Symbols
Upstream Line Protection (Slow Path):        0.0 DMT Symbols
Downstream delay:                            1.9 ms
Upstream delay:                              1.9 ms
Tx total power :                             7.7 dbm
FE Tx total power :                          6.0 dbm
VDSL Estimated Loop Length :                 16 ft
G.Hs Estimated Near End Loop Length :        5 ft
G.Hs Estimated Far End Loop Length :         0 ft
Current framing mode:                        0x80
Far end capabilities mask:                   0x00
SNR Margin:                                  5.3 dB
Attenuation:                                 16.8 dB
Avg SNR Margin:                              6.3 dB
Avg SNR:                                     32.9 dB
Console#show lre rate-info 1/1
port 1 Rate informaition :
Downstream line rate:                  119040 kbps
Upstream line rate:                    115648 kbps
Fast Downstream payload rate:          0 kbps
Slow Downstream payload rate:          104960 kbps
Fast Upstream payload rate:            0 kbps
Slow Upstream payload rate:            101952 kbps
Downstream attainable payload rate:    110080 kbps
Downstream attainable line rate:       129664 kbps
Upstream attainable payload rate:      109696 kbps
Upstream attainable line rate:         124480 kbps
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying VDSL Performance Statistics

This section describes the performance information displayed for VDSL lines, including common error conditions over predefined intervals.

Field Attributes

Error Statistics

Table 10-3 Error Statistics

Parameter	Description
Loss of Frame	Number of seconds during which there was loss of framing
Loss of Signal	Number of seconds during which there was loss of signal
Loss of Power	Number of seconds during which there was loss of power
Errored Seconds	Number of seconds during which there was one or more CRC anomalies, or one or more Loss of Signal (LOS) or Loss of Framing (LOF) defects
Severely Errored Seconds	Number of seconds containing 18 or more CRC-8 anomalies, one or more Loss of Signal (LOS) defects, one or more Severely Errored Frame (SEF) defects, or one or more Loss of Power (LPR) defects.
Unavailable Seconds	Number of seconds during which the VDSL transceiver is powered up but not available.

Ethernet Receive Performance Counters

Table 10-4 Ethernet Receive Performance Counters

Parameter	Description
Frames	Number of frames (bad, broadcast and multicast) received.
Bytes	Number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Dropped Frames	Number of events in which frames were dropped due to lack of resources.

Downloaded from www.Manualslib.com manuals search engine

Table 10-4 Ethernet Receive Performance Counters (Continued)

Parameter	Description
Alignment Errors	Number of alignment errors (missynchronized data packets).
Oversize	Number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Undersize	Number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
CRC Errors	Number of CRC errors (FCS or alignment errors).
Carrier Sense Errors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.

Ethernet Transmit Performance Counters

Table 10-5 Ethernet Transmit Performance Counters

Parameter	Description
Frames	Number of frames (unicast, broadcast and multicast) transmitted.
Bytes	Number of bytes of data transmitted onto the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Pause Frames	Number of MAC Control frames transmitted with an opcode indicating the PAUSE operation.

Downloaded from www.Manualslib.com manuals search engine

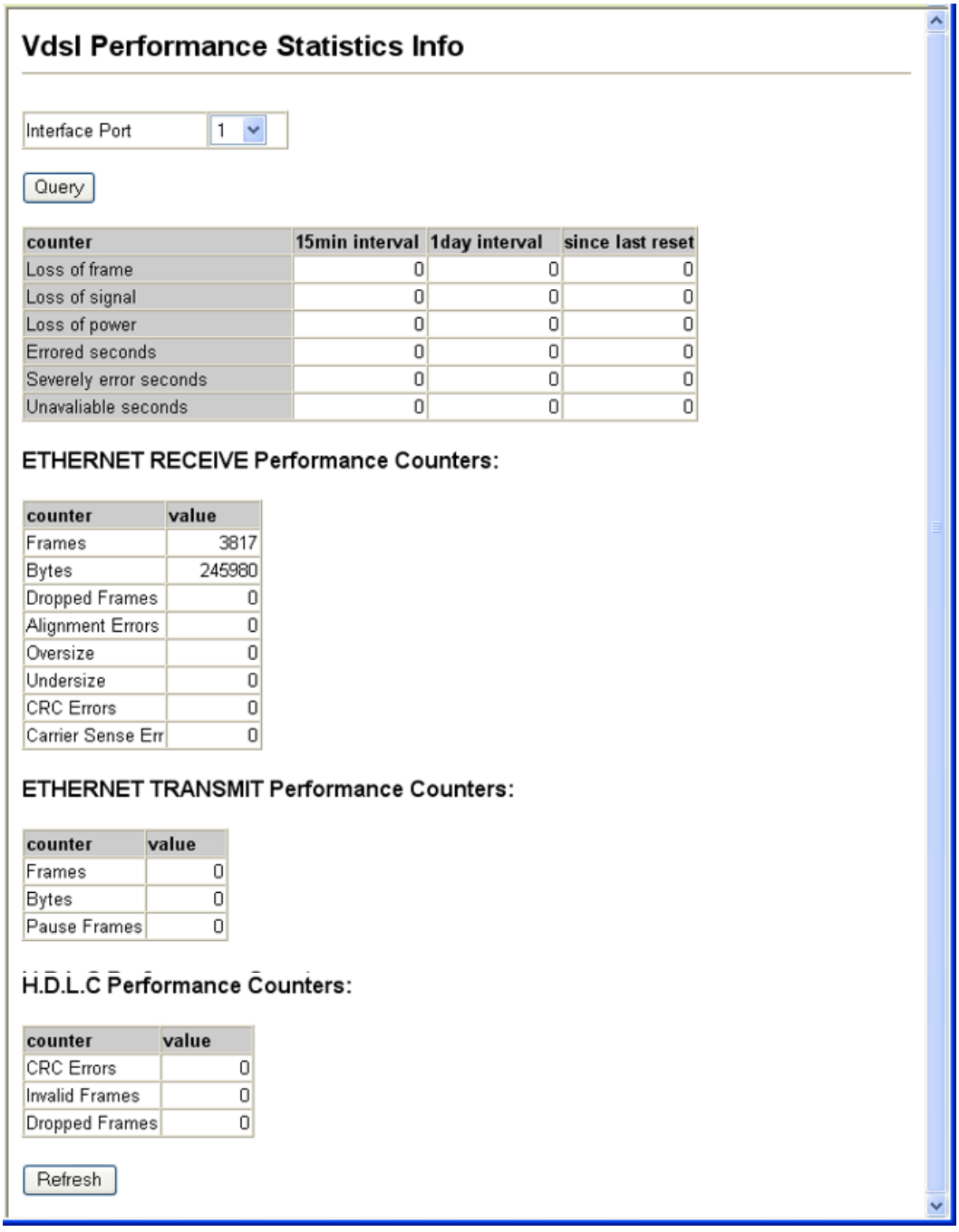
High-Level Data-Link Control (H.D.L.C.) Performance Counters

Table 10-6 H.D.L.C. Performance Counters

Parameter	Description
CRC Errors	Number of CRC errors (FCS or alignment errors).
Invalid Frames	Number of frames not properly bounded by flags, not containing an integral number of octets prior to zero-bit insertion or following zero-bit extraction, containing an FCS error, or containing an incorrect address field.
Dropped Frames	Number of frames dropped due to lack of resources.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, VDSL Performance Statistics. Select a VDSL port from the drop-down list, and click Query.



Vdsl Performance Statistics Info

Interface Port 1

Query

counter	15min interval	1day interval	since last reset
Loss of frame	0	0	0
Loss of signal	0	0	0
Loss of power	0	0	0
Errored seconds	0	0	0
Severely error seconds	0	0	0
Unavaliable seconds	0	0	0

ETHERNET RECEIVE Performance Counters:

counter	value
Frames	3817
Bytes	245980
Dropped Frames	0
Alignment Errors	0
Oversize	0
Undersize	0
CRC Errors	0
Carrier Sense Err	0

ETHERNET TRANSMIT Performance Counters:

counter	value
Frames	0
Bytes	0
Pause Frames	0

H.D.L.C Performance Counters:

counter	value
CRC Errors	0
Invalid Frames	0
Dropped Frames	0

Refresh

Figure 10-5 VDSL Performance Statistics

Downloaded from www.Manualslib.com manuals search engine

CLI – This example displays performance information for the selected VDSL port.

```
Console#show lre perf 1/1                                          29-82
port 1 performance counters since last reset :
Loss of frame : 0              Loss of signal :        0
Loss of power : 0              Errored seconds :       17
Severely error seconds: 0      Unavaliable seconds :   0

port 1 performance counters in current 15min interval :
Loss of frame : 0              Loss of signal :        0
Loss of power : 0              Errored seconds :       4
Severely error seconds: 0      Unavaliable seconds :   0

port 1 performance counters in current 1day interval :
Loss of frame : 0              Loss of signal :        0
Loss of power : 0              Errored seconds :       13
Severely error seconds: 0      Unavaliable seconds :   0

port 1/14 ETHERNET RECEIVE Performance Counters :
Frames :                2835   Bytes :                 3385891280
Pause Frames :          24     Broadcast Frames :      0
Dropped Frames :        0      Alignment Errors :      0
Oversize :              0      Undersize :             0
CRC Errors :            0      Carrier Sense Err :     0

port 1/14 ETHERNET TRANSMIT Performance Counters :
Frames :                3048   Bytes :                 3385891280
Pause Frames :          0

port 1/14 H.D.L.C Performance Counters :
CRC Errors :            3385891280     Invalid Frames :        0
Dropped Frames :        0

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring an Alarm Profile

This section describes how to configure a list of threshold values for error states which can be applied to a selected group of ports.

Command Attributes

- **Alarm Profile** – Name of the profile. (Range: 1-31 alphanumeric characters)

  The default profile includes the default thresholds for VDSL lines.

- **thresh-15min-ess** – Threshold for Errored Seconds (ESs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 2)

  An Errored Second is a one-second interval containing one or more CRC anomalies, or one or more Loss of Signal (LOS) or Loss of Framing (LOF) defects.

  This parameter sets the threshold for the number of errored seconds within any 15 minute collection interval for performance data. If the number of errored seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfESsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

  When this threshold is exceeded, notification messages are sent to registered SNMP hosts as required by RFC 3728, reported to the syslog system, and displayed on the console interface.

- **thresh-15min-sess** – Threshold for Severely Errored Seconds (SESs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 2)

  A Severely Errored Second is a one-second interval containing 18 or more CRC-8 anomalies, one or more Loss of Signal (LOS) defects, one or more Severely Errored Frame (SEF) defects, or one or more Loss of Power (LPR) defects.

Downloaded from www.Manualslib.com manuals search engine

This parameter sets the threshold for the number of severely errored seconds within any 15 minute collection interval for performance data. If the number of severely errored seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfSESsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

- **thresh-15min-lofs** – Threshold for Loss of Frame seconds (LOFs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 10)

  This parameter sets the threshold for the number of seconds during which there is loss of framing within any 15 minute collection interval for performance data. If loss of framing in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLofsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

- **thresh-15min-lols** – Threshold for Loss of Link seconds (LOLs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 10)

  This parameter sets the threshold for the number of seconds during which there is loss of link within any 15 minute collection interval for performance data. If loss of link in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLolsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

- **thresh-15min-loss** – Threshold for Loss of Signal seconds (LOSs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 2)

  This parameter sets the threshold for the number of seconds during which there is loss of signal within any 15 minute collection interval for performance data. If loss of signal in a particular 15-minute collection

Downloaded from www.Manualslib.com manuals search engine

interval reaches or exceeds this value, a vdslPerfLossThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

- **thresh-15min-uass** – Threshold for Unavailable Seconds (UASs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 10)

  An Unavailable Seconds is a one-second interval during which the VDSL transceiver is powered up but not available (i.e., not in the Showtime state). A VDSL line will become unavailable at the onset of 10 contiguous Severely Errored Seconds. Once unavailable, the line should become available at the onset of 10 contiguous seconds with no SESs.

  This parameter sets the threshold for the number of severely errored seconds within any 15 minute collection interval for performance data. If the number of severely errored seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfUASsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

- **thresh-15min-lprs** – Threshold for Loss of Power Seconds (LPRs) that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 10)

  This parameter sets the threshold for the number of loss of power seconds within any 15 minute collection interval for performance data. If the number of loss of power seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLprsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Downloaded from www.Manualslib.com manuals search engine

- **init-failure** – Threshold for initialization failures that can occur within any given 15 minutes. (Range: 0-900 seconds, where 0 disables the threshold; Default: 1)

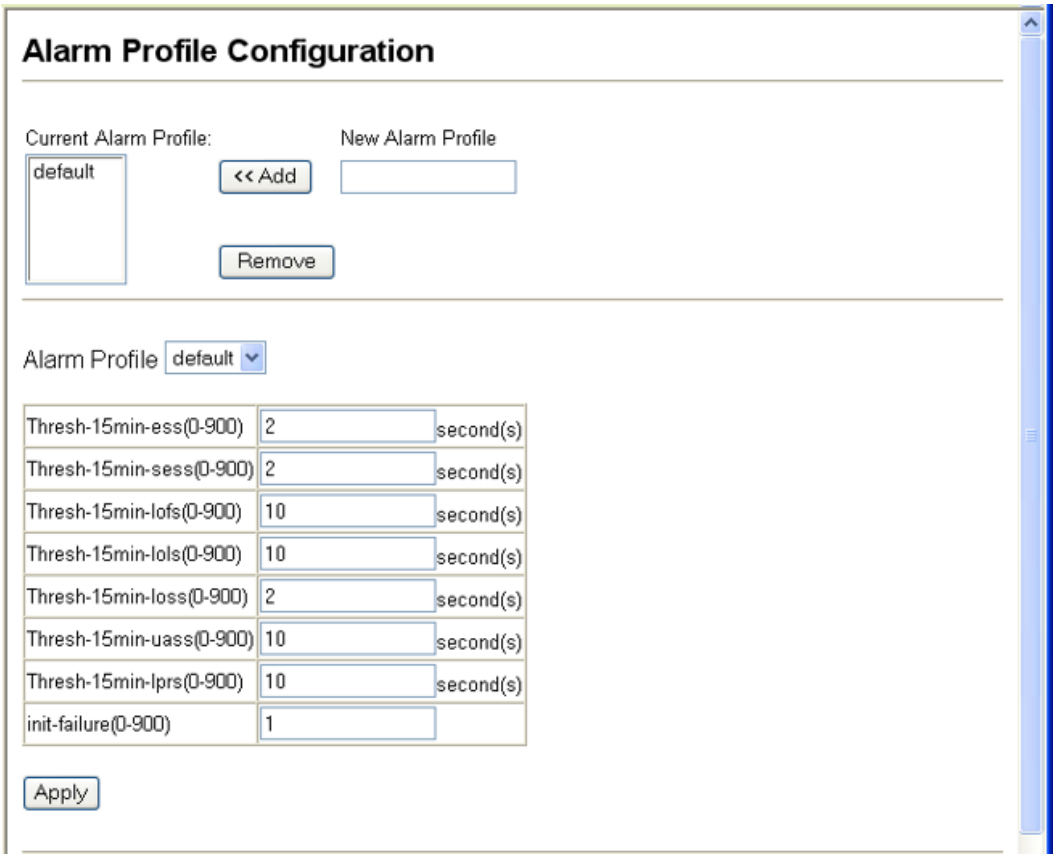
  There are many factors which can cause an initialization failure, including lossOfFraming, lossOfSignal, lossOfPower, lossOfSignalQuality, lossOfLink, dataInitFailure, configInitFailure, protocolInitFailure, or noPeerVtuPresent. All outstanding error conditions associated with a VDSL transceiver are defined by the vdslPhysCurrStatus bitmask in RFC 3728. However, note that since the status of remote transceivers is obtained via the embedded operation channel (EOC), this information may be unavailable for units that are unreachable via the EOC during a line error condition. Therefore, not all conditions may always be included in its current status.

  This parameter sets the threshold for the number of initialization failures within any 15 minute collection interval for performance data. If the number of initialization failures in a particular 15-minute collection interval reaches or exceeds this value, a vdslInitFailureNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

- **Alarm Profile Mapping** – Applies an alarm profile to the selected VDSL ports.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, Alarm Profile Configuration. Select a profile from the drop-down list above the Alarm Profile table of thresholds, configure the required items in this table, and then click the Apply button beneath the table to store the profile settings. Now select the required alarm profile from the drop-down list in the Alarm Profile Mapping table, and click the Apply button next to the VDSL ports to apply the selected profile.



Downloaded from www.Manualslib.com manuals search engine

Figure 10-6 Alarm Profile Configuration

CLI – This example displays sample settings for an alarm profile.

```
Console(config)#alarm-profile southport                    29-52
Console(config-alarm-profile)#thresh-15min-ess 25          29-54
Console(config-alarm-profile)#thresh-15min-sess 15         29-59
Console(config-alarm-profile)#thresh-15min-lofs 15         29-55
Console(config-alarm-profile)#thresh-15min-lols 15         29-56
Console(config-alarm-profile)#thresh-15min-loss 15         29-57
Console(config-alarm-profile)#thresh-15min-uass 15         29-60
Console(config-alarm-profile)#thresh-15min-lprs 15         29-58
Console(config-alarm-profile)#init-failure 5               29-53
Console(config-line-profile)#exit
Console(config)#interface ethernet 1/1                     25-13
Console(config-if)#lre alarm-profile southport             29-52
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying CPE Information

This section describes the information displayed for an attached CPE, including firmware module versions, and performance counters.

Field Attributes

CPE Firmware Versions

Table 10-7 CPE Firmware Versions

Parameter	Description
Protocol	Manufacturer ID, version numbers, and vendor ID
Host Application Version	Primary application firmware version
BME Firmware Version	Burst Mode Engine (DSP) firmware version
AFE Hardware Version	Analog Front End (DA/AD converter) hardware version
IFE Hardware Version	Integrated Front End (Port VDSL filtering) hardware version
Firmware Number	The number of firmware versions stored in this device.
Active Version	The firmware version currently in used by this device.
verId	The identifiers for the stored firmware versions.
CO Firmware Buffer	Status of the firmware download buffer.

CO Firmware Buffer Information

Table 10-8 CO Firmware Buffer Information

Parameter	Description
Valid	Whether or not the downloaded firmware is valid.
Firmware Size	The size of the firmware stored in the buffer.
Firmware Version	The firmware version number.

Downloaded from www.Manualslib.com manuals search engine

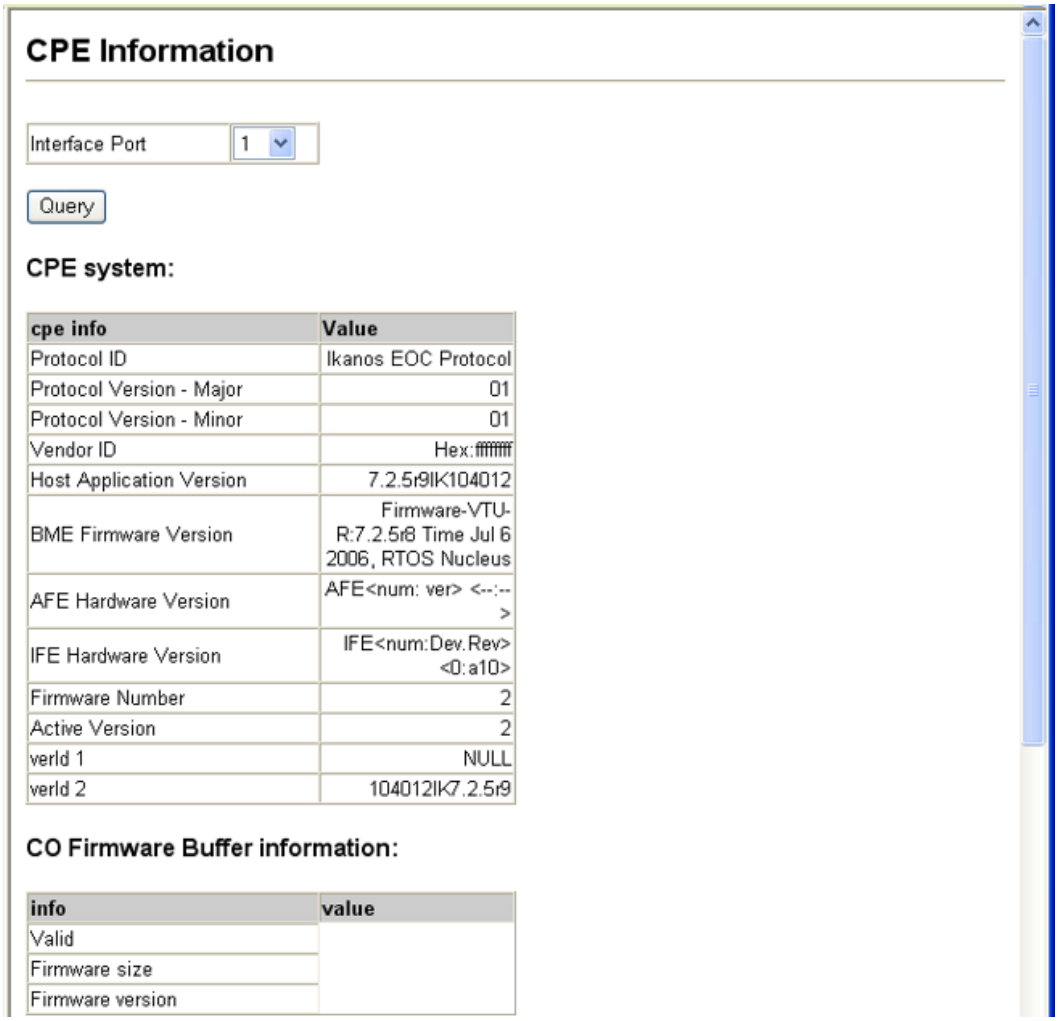
CPE Performance Counters

Table 10-9 CPE Performance Counters

Parameter	Description
cpe performance counters	
FeFEC_F	Far end Forward Error Correction on fast path
FeCRC_F	Far end CRC errors on fast path
FeFEC_S	Far end Forward Error Correction on slow path
FeCRC_S	Far end CRC errors on slow path
FeFLOS	Far end Loss of Signal
FeSEF	Far end Severely Errored Frame
FeFECUnCrr_F	Far end Forward Error Correction on fast path - uncorrected errors
FeFECUnCrr_S	Far end Forward Error Correction on slow path - uncorrected errors
INI Far End Counters (Ikanos Network Interface)	
TX_FRAME_CNT	Transmitted frame count
RX_FRAME_CNT	Received frame count
TX_CRC_FRAME_CNT	Transmitted frames with CRC errors
RX_CRC_FRAME_CNT	Received frames with CRC errors
DROP_FRAME_CNT	Frames dropped due to data errors or buffer overflow.
Error Seconds	A one-second interval containing one or more CRC anomalies, or one or more Loss of Signal (LOS) or Loss of Framing (LOF) defects
VDSL Port CRS Errors	CRC errors on the VDSL port
SNR Margin and Attenuation	
SNR Margin	Current signal-to-noise margin
Attenuation	Amount of attenuation in signal strength

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, CPE Information. Select a VDSL port from the drop-down list, and click Query.



CPE Information

Interface Port 1

Query

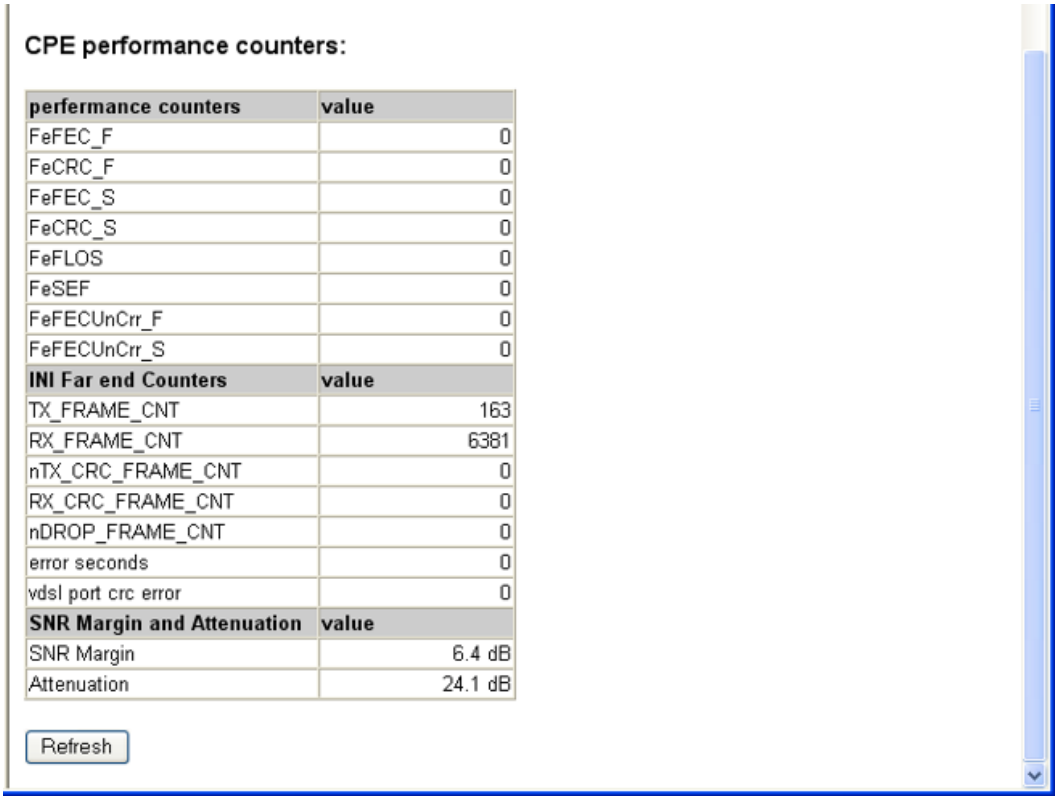
CPE system:

cpe info	Value
Protocol ID	Ikanos EOC Protocol
Protocol Version - Major	01
Protocol Version - Minor	01
Vendor ID	Hex:ffffffff
Host Application Version	7.2.5r9IK104012
BME Firmware Version	Firmware-VTU-R:7.2.5r8 Time Jul 6 2006, RTOS Nucleus
AFE Hardware Version	AFE<num: ver> <--:-->
IFE Hardware Version	IFE<num:Dev.Rev> <0:a10>
Firmware Number	2
Active Version	2
verId 1	NULL
verId 2	104012IK7.2.5r9

CO Firmware Buffer information:

info	value
Valid	
Firmware size	
Firmware version	

Downloaded from www.Manualslib.com manuals search engine



CPE performance counters:

perfermance counters	value
FeFEC_F	0
FeCRC_F	0
FeFEC_S	0
FeCRC_S	0
FeFLOS	0
FeSEF	0
FeFECUnCrr_F	0
FeFECUnCrr_S	0
INI Far end Counters	**value**
TX_FRAME_CNT	163
RX_FRAME_CNT	6381
nTX_CRC_FRAME_CNT	0
RX_CRC_FRAME_CNT	0
nDROP_FRAME_CNT	0
error seconds	0
vdsl port crc error	0
SNR Margin and Attenuation	**value**
SNR Margin	6.4 dB
Attenuation	24.1 dB

Refresh

Figure 10-7 CPE Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This example displays information about the CPE attached to the selected VDSL port.

```
Console#show cpe-info 1/1
Protocol ID:    Ikanos EOC Protocol
Protocol Version - Major:       01
Protocol Version - Minor:       01
Vendor ID (Value):      ffffffff (HEX), -1 (DECIMAL)
Host Application Version:     7.2.5r7IK104012
BME Firmware Version:           Firmware-VTU-R:7.2.5r7 Time May 19 2006,
RTOS Nucleus
AFE Hardware Version:         AFE<num: ver> <--:-->
IFE Hardware Version:         IFE<num:Dev.Rev> <0:a10>

Firmware Number:                2
Active Version:                 2
verId 1:                        NULL
verId 2:                        104012IK7.2.5r9

CO Firmware Buffer is empty now
Console#show cpe performance counter 1/1
port 1 The cpe perfermance counters are as below:
FeFEC_F:                0               FeCRC_F:        0
FeFEC_S:                0               FeCRC_S:        0
FeFLOS:                 0               FeSEF:  0
FeFECUnCrr_F:           0               FeFECUnCrr_S:   0

port 1 INI Far end Counters are as below:
TX_FRAME_CNT:           113
RX_FRAME_CNT:           346
TX_CRC_FRAME_CNT:       0
RX_CRC_FRAME_CNT:       0
DROP_FRAME_CNT:         0
SNR Margin:             6.2 dB
Attenuation:            24.5 dB
error seconds :         43
vdsl port crc error :   0
Console(config-if)#
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring OAM Functions and Upgrading CPE Firmware

This section describes operation and maintenance (OAM) functions for remote customer premises equipment (CPE), such as clearing counters, enabling loopback testing, and upgrading firmware.

Command Usage

Upgrading CPE Firmware

To upgrade firmware on a CPE follow these steps:

1. Use the "Copy BME Firmware to CO Firmware Buffer from TFTP Server" dialog box to download firmware from a TFTP server to reserved buffer space in the switch.
2. Under the OAM Remote Action field, click "Upgrade Firmware" to transfer the firmware to a remote CPE.
3. Under the OAM Remote Action field, click "Firmware Active" to activate the new firmware.

Command Attributes

Local OAM Functions

- **Clear Counter** – Clears statistical data (in the VDSL chip) for a specified VDSL port.

  The default profile includes the default thresholds for VDSL lines.

  For information on the type of statistics maintained by the VDSL chip, see the "Displaying VDSL Performance Statistics" on page 10-25.
- **Loopback Test** – Conducts a loopback test between the specified VDSL port and the attached CPE.

  This command checks the link by transmitting a test signal (IEEE 802.3ah OAM PDU) from the specified VDSL port to the attached

Downloaded from www.Manualslib.com manuals search engine

CPE, and verifying that the signal is returned from the CPE without any errors.

Upgrading CPE Firmware

- **Upgrade Firmware** – Transfers firmware from reserved buffer space in the switch to a remote CPE.
- **Firmware Active** – Activates the alternate (inactive) BME firmware version on the CPE. (BME indicates the Burst Mode Engine used for digital signal processing.)

Copying CPE Firmware to Buffer on Switch

- **Copy BME Firmware to CO Firmware Buffer from TFTP Server** – Copies BME firmware used for upgrading CPEs from a TFTP server to reserved buffer space in the switch.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VDSL, VDSL OAM. Select a VDSL port from the drop-down list, and perform any of the local or remote OAM functions listed under the Action field. Before upgrading firmware on an attached CPE, first download it to the reserved buffer space on the switch using the dialog box at the bottom of this screen.

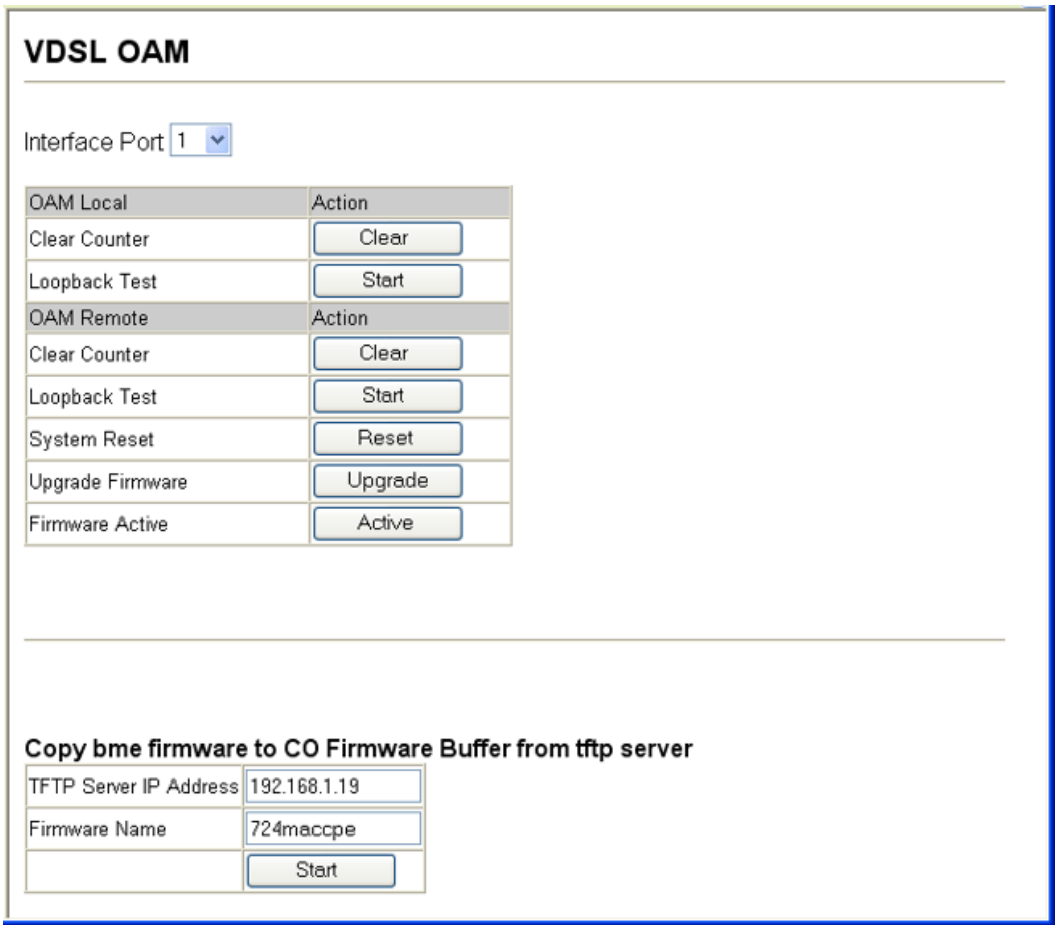


Figure 10-8 CPE Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows how to perform common OAM functions, and how to download firmware to a CPE.

```
Console(config)#interface ethernet 1/1                          25-13
Console(config-if)#oam local clear counter                      29-86
port 1 :        success to clear perfermance counters!
Console(config-if)#exit
Console#copy tftp firmware                                      29-87
TFTP server IP address: 192.168.1.19
Source file name: 724maccpe
Success.
Firmware size :         485719
Firmware version :      104012IK7.2.4r9_Back_to_Back_Mac
Console(config)#interface ethernet 1/1
Console(config-if)#oam remote upgrade firmware                  29-90
Console(config-if)#oam remote firmware active                   29-90
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 11
ADDRESS TABLE SETTINGS

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts**[12] – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

12. Web Only.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.

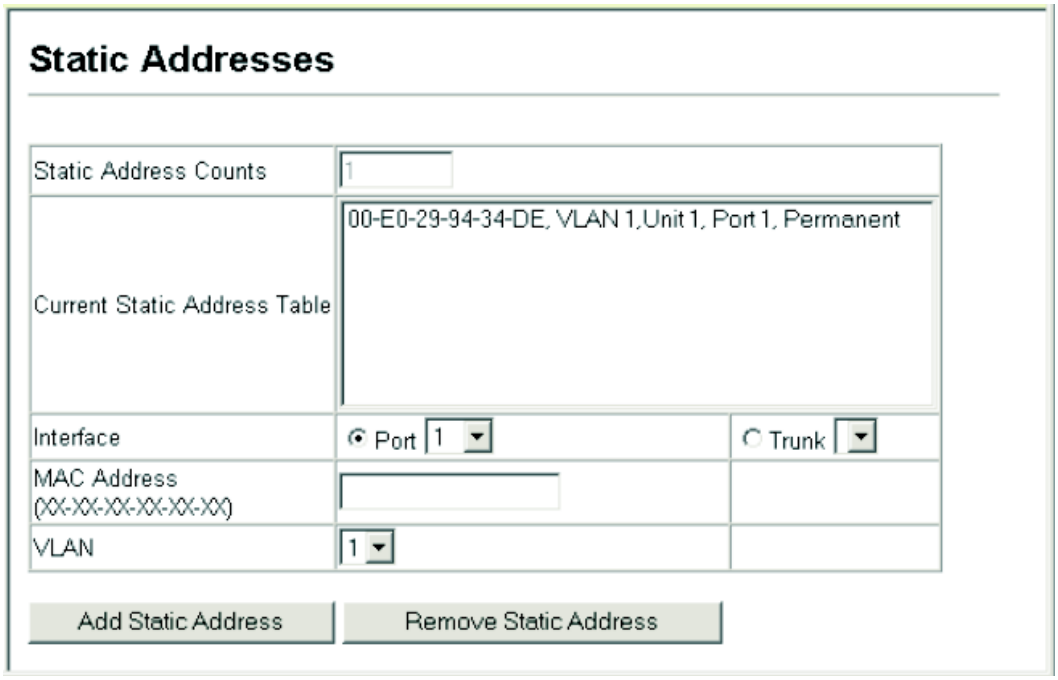


Figure 11-1 Static Addresses

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
  interface ethernet 1/1 vlan 1 delete-on-reset                30-2
Console(config)#
```

Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4094).
- **Address Table Sort Key** – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.

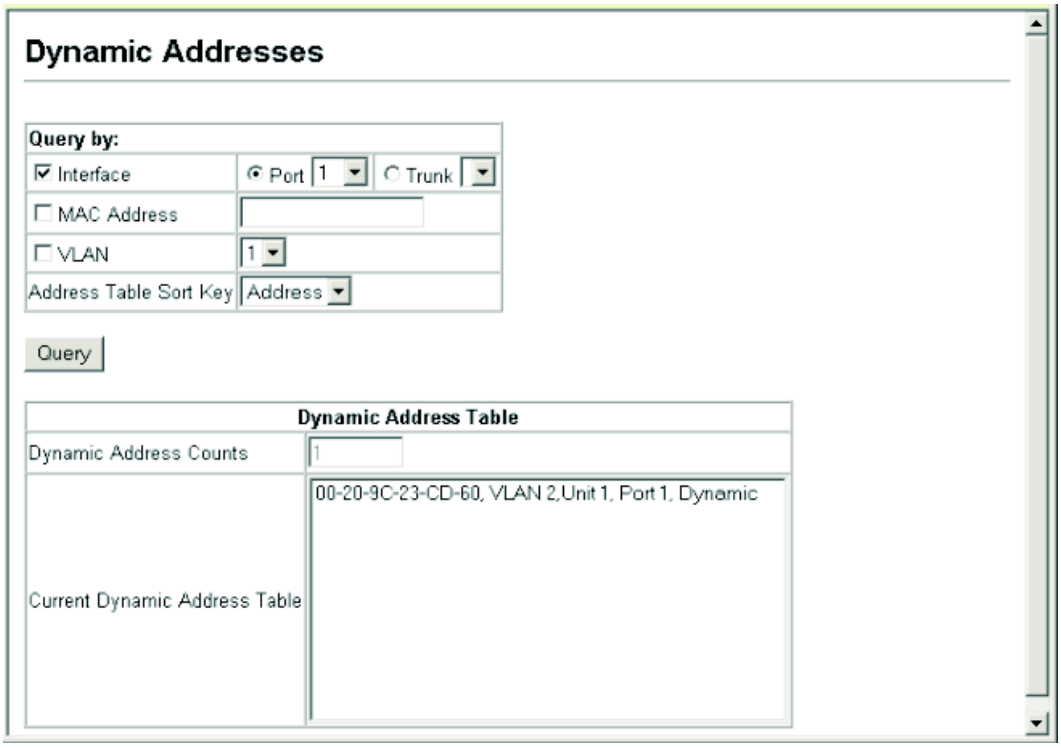


Figure 11-2 Dynamic Addresses

Downloaded from www.Manualslib.com manuals search engine

CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1          30-4
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- **Aging Status** – Enables/disables the aging function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.

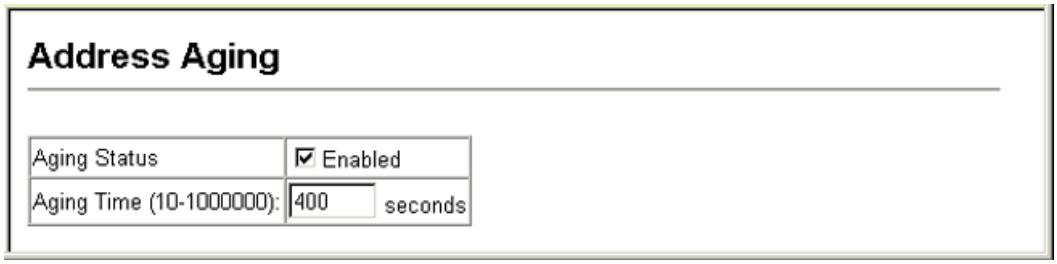


Figure 11-3 Address Aging

CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400               30-5
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 12
SPANNING TREE ALGORITHM

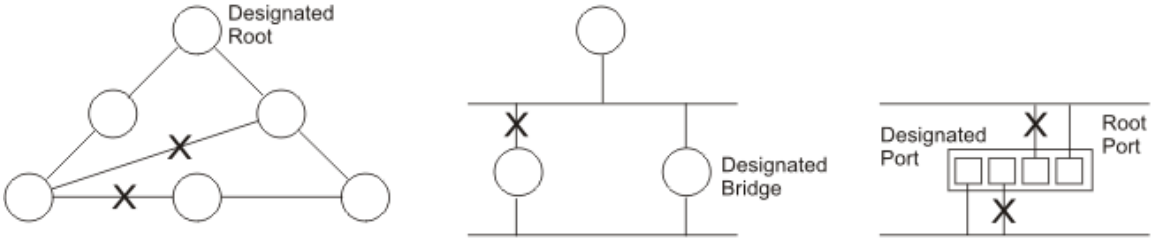
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Downloaded from www.Manualslib.com manuals search engine



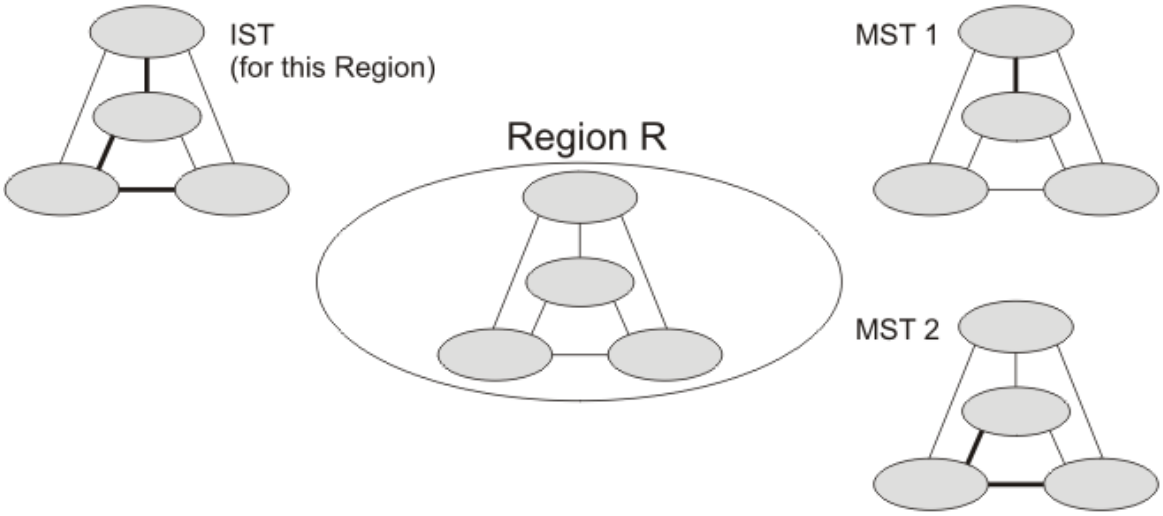
Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves must faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

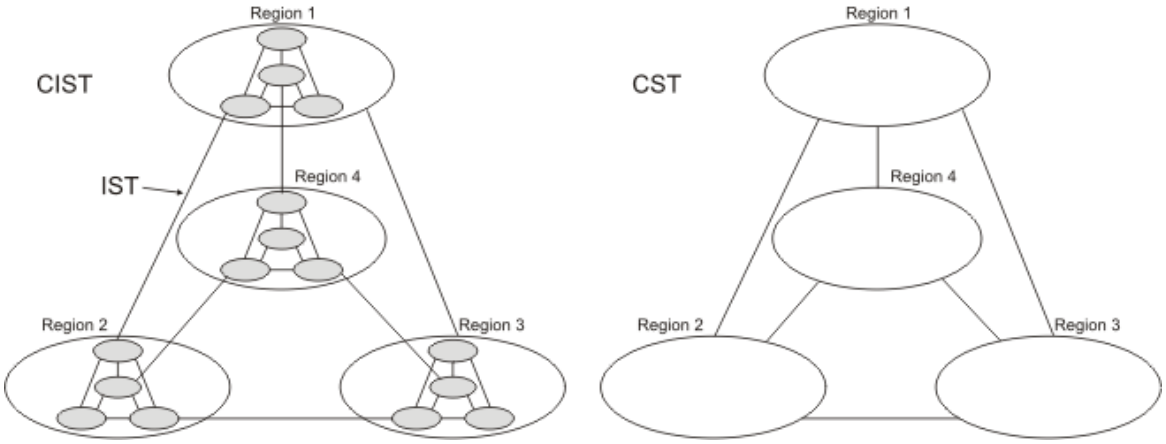
MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to

Downloaded from www.Manualslib.com manuals search engine

maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.



An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including the Region Name, Revision Level and Configuration Digest – see "Configuring Multiple Spanning Trees" on page 12-22). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.



Downloaded from www.Manualslib.com manuals search engine

MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree mode is set to MSTP (page 12-8), and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would

Downloaded from www.Manualslib.com manuals search engine

make it return to a discarding state; otherwise, temporary data loops might result.

- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
  - **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
  - **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

These additional parameters are only displayed for the CLI:

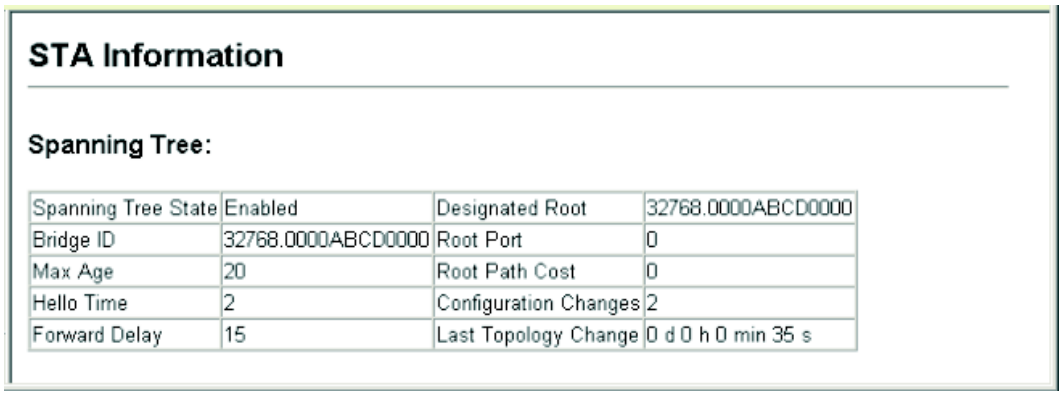
- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D)
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- **Instance** – Instance identifier of this spanning tree. (This is always 0 for the CIST.)
- **VLANs configuration** – VLANs assigned to the CIST.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive

Downloaded from www.Manualslib.com manuals search engine

configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Max hops** – The max number of hop counts for the MST region.
- **Remaining hops** – The remaining number of hop counts for the MST instance.
- **Transmission limit** – The minimum interval between the transmission of consecutive RSTP/MSTP BPDUs.
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

Figure 12-1 STA Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree                                        31-25
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode:                MSTP
 Spanning tree enable/disable:      enable
 Instance:                          0
 Vlans configuration:               1-4093
 Priority:                          32768
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Max hops:                          20
 Remaining hops:                    20
 Designated Root                    32768.0.0000ABCD0000
 Current root port:                 1
 Current root cost                  200000
 Number of topology changes:        1
 Last topology changes time (sec.): 13380
 Transmission limit:                3
 Path Cost Method:                  long

---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
 Admin status:             enabled
 Role:                     disable
 State:                    discarding
 External admin path cost: 10000
 Internal admin cost:      10000
 External oper path cost:  10000
 Internal oper path cost:  10000
 Priority:                 128
 Designated cost:          300000
 Designated port:          128.1
 Designated root:          32768.0000E8AAAA00
 Designated bridge:        32768.0030F1D473A0
 Fast forwarding:          disabled
 Forward transitions:      0
 Admin edge port:          disabled
 Oper edge port:           disabled
 Admin Link type:          auto
 Oper Link type:           point-to-point
 Spanning Tree Status:     enabled
:
:
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Downloaded from www.Manualslib.com manuals search engine

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol[13]
  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.
- Rapid Spanning Tree Protocol[13]
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
- Multiple Spanning Tree Protocol
  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

13. STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

Downloaded from www.Manualslib.com manuals search engine

- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to

Downloaded from www.Manualslib.com manuals search engine

reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)

- Default: 20
- Minimum: The higher of 6 or [2 x (Hello Time + 1)].
- Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

Configuration Settings for RSTP

The following attributes apply to both RSTP and MSTP:

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Downloaded from www.Manualslib.com manuals search engine

Configuration Settings for MSTP

- **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned. (Default: 33)
- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- **Region Revision**[14] – The revision for this MSTI. (Range: 0-65535; Default: 0)
- **Region Name**[14] – The name for this MSTI. (Maximum length: 32 characters)
- **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

14. The MST name and revision number are both required to uniquely identify an MST region.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, and click Apply.

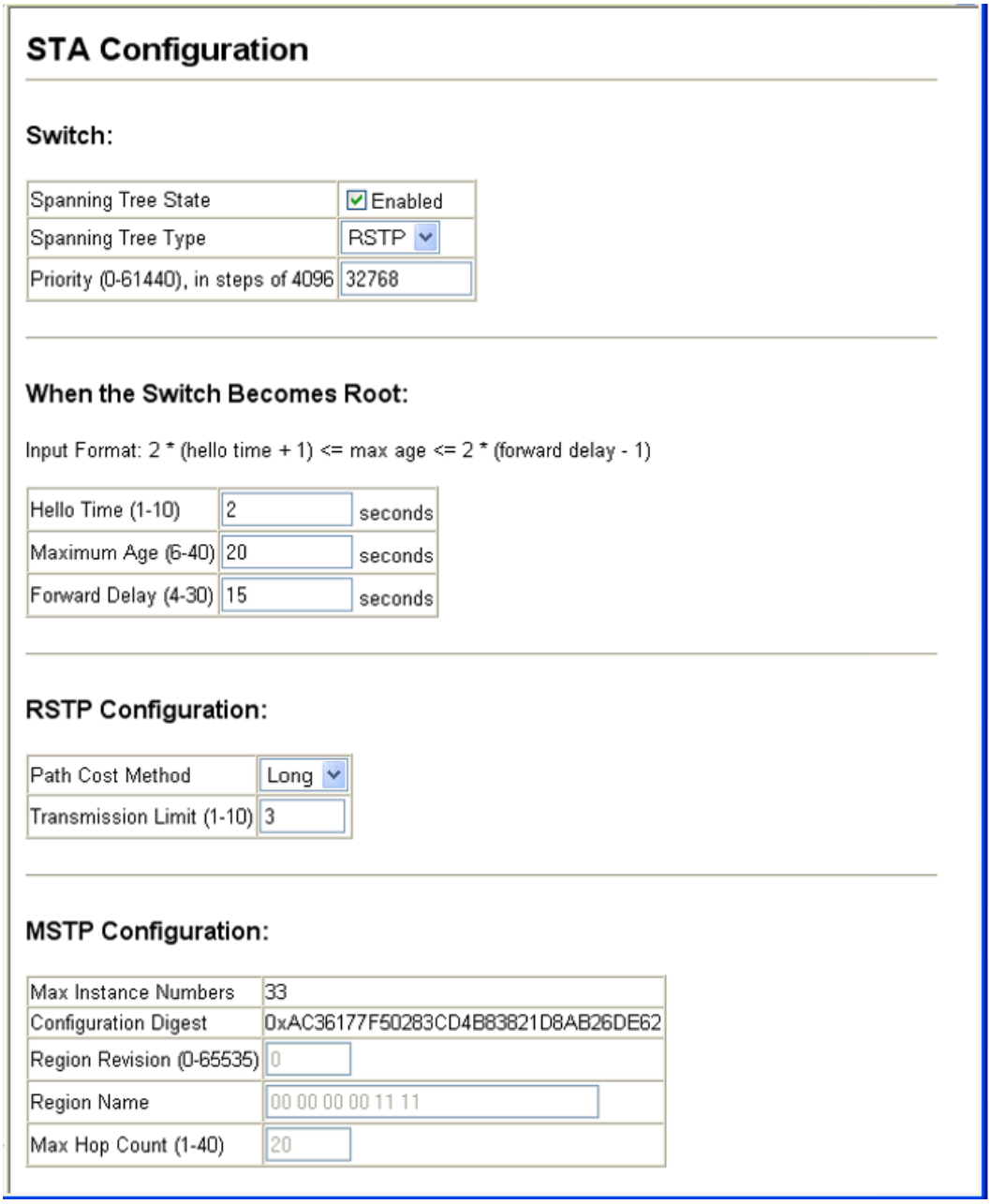


Figure 12-2 STA Global Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This example enables Spanning Tree Protocol, sets the mode to MST, and then configures the STA and MSTP parameters.

```
Console(config)#spanning-tree                                  31-3
Console(config)#spanning-tree mode mstp                        31-4
Console(config)#spanning-tree priority 40000                   31-8
Console(config)#spanning-tree hello-time 5                     31-6
Console(config)#spanning-tree max-age 38                       31-7
Console(config)#spanning-tree forward-time 20                  31-5
Console(config)#spanning-tree pathcost method long             31-9
Console(config)#spanning-tree transmission-limit 4             31-10
Console(config)#spanning-tree mst-configuration                31-10
Console(config-mstp)#revision 1                                31-14
Console(config-mstp)#name R&D                                  31-13
Console(config-mstp)#max-hops 30                               31-14
Console(config-mstp)#
```

Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

Field Attributes

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

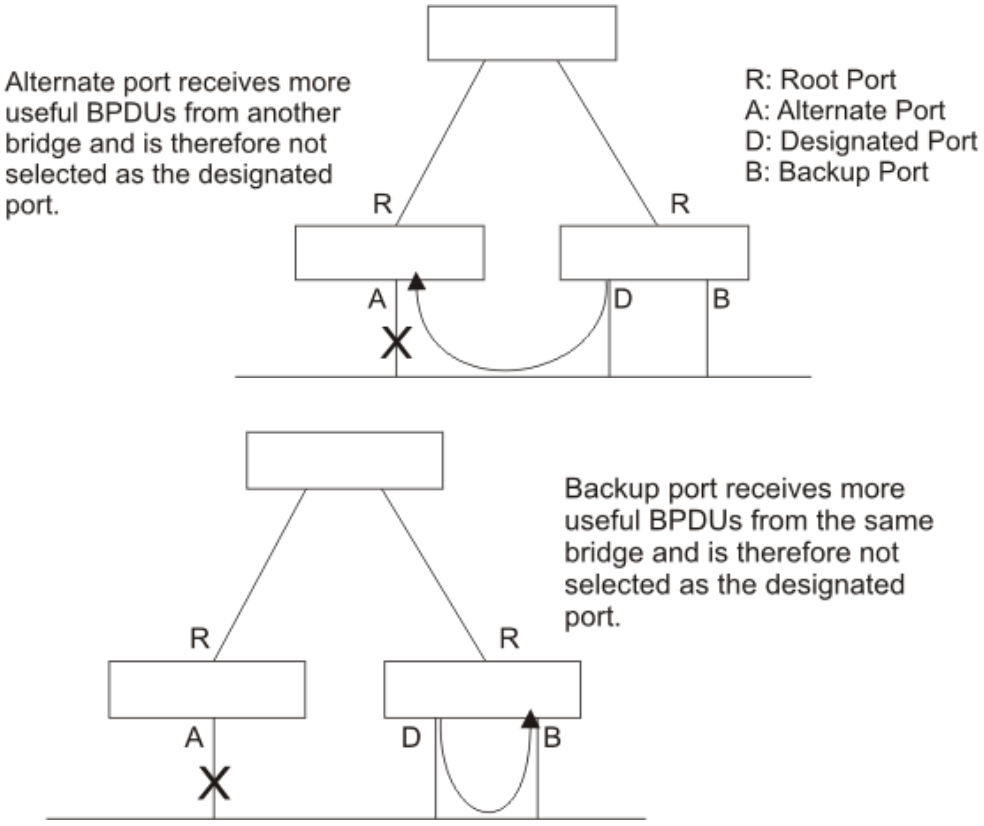
    The rules defining port status are:

    - A port on a network segment with no other STA compliant bridging device is always forwarding.

Downloaded from www.Manualslib.com manuals search engine

  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 12-18.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 12-18 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), or is the MSTI regional root (i.e., **master** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

Downloaded from www.Manualslib.com manuals search engine



- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- **External path cost** – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Internal path cost** – The path cost for the MST. See the preceding item.
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network

Downloaded from www.Manualslib.com manuals search engine

loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA, Port Information or STA Trunk Information.

STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	3	0	32768.0.000012338976	128.1	100000	Point-to-Point	Disabled	Designated	
2	Enabled	Forwarding	5	0	32768.0.000012338976	128.2	100000	Point-to-Point	Disabled	Designated	
3	Enabled	Discarding	0	0	32768.0.000012338976	128.3	100000	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	0	32768.0.000012338976	128.4	100000	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	0	32768.0.000012338976	128.5	100000	Point-to-Point	Disabled	Disabled	
6	Enabled	Discarding	0	0	32768.0.000012338976	128.6	100000	Point-to-Point	Disabled	Disabled	
7	Enabled	Discarding	0	0	32768.0.000012338976	128.7	100000	Point-to-Point	Disabled	Disabled	
8	Enabled	Discarding	0	0	32768.0.000012338976	128.8	100000	Point-to-Point	Disabled	Disabled	
9	Enabled	Discarding	0	0	32768.0.000012338976	128.9	100000	Point-to-Point	Disabled	Disabled	
10	Enabled	Discarding	0	0	32768.0.000012338976	128.10	100000	Point-to-Point	Disabled	Disabled	

Figure 12-3 STA Port Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/5                          31-25
Eth  1/ 5 information
---------------------------------------------------------------------
 Admin Status:             Enabled
 Role:                     Disabled
 State:                    Discarding
 External Admin Path Cost: 100000
 Internal Admin Path Cost: 100000
 External Oper Path Cost:  100000
 Internal Oper Path Cost:  100000
 Priority:                 128
 Designated Cost:          0
 Designated Port:          128.1
 Designated Root:          32768.0.000000001111
 Designated Bridge:        32768.0.000000001111
 Fast Forwarding:          Disabled
 Forward transitions:      2
 Admin Edge Port:          Disabled
 Oper Edge Port:           Disabled
 Admin Link Type:          Auto
 Oper Link Type:           Point-to-point
 Spanning Tree Status:     Enabled

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Interface Settings

You can configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 12-13 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, continues learning addresses.
- **Trunk**[15] – Indicates if a port is a member of a trunk.

The following interface attributes can be configured:

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network

15. STA Port Configuration only

Downloaded from www.Manualslib.com manuals search engine

loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

- Default: 128
- Range: 0-240, in steps of 16

- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) (Range: 0 for auto-configuration, 1-65535 for the short path cost method[16], 1-200,000,000 for the long path cost method)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 12-1 Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 12-2 Recommended STA Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001*
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

* Default path costs use the IEEE 802.1w-2001 recommendations, except when short path cost method is selected and the recommended value would fall below 65,535 (i.e., the minimum default setting).

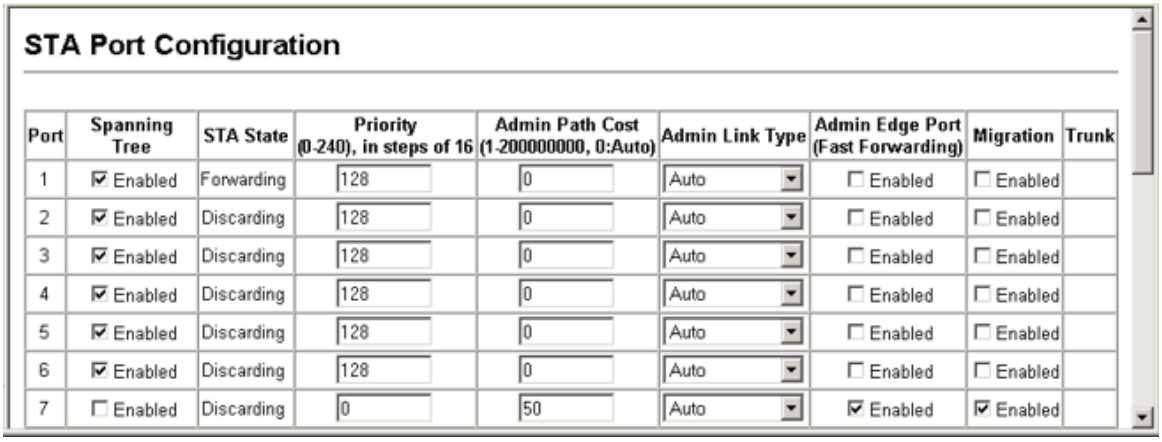
16. Refer to "Configuring Global Settings" on page 12-8 for information on setting the path cost method.

Downloaded from www.Manualslib.com manuals search engine

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port** (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Downloaded from www.Manualslib.com manuals search engine

Web – Click Spanning Tree, STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.



STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Admin Path Cost (1-200000000, 0:Auto)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	☑ Enabled	Forwarding	128	0	Auto	☐ Enabled	☐ Enabled	
2	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
3	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
4	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
5	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
6	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
7	☐ Enabled	Discarding	0	50	Auto	☑ Enabled	☑ Enabled	

Figure 12-4 STA Port Configuration

CLI – This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7                          25-2
Console(config-if)#no spanning-tree spanning-disabled           31-15
Console(config-if)#spanning-tree port-priority 0                31-18
Console(config-if)#spanning-tree cost 50                        31-16
Console(config-if)#spanning-tree link-type auto                 31-21
Console(config-if)#no spanning-tree edge-port                   31-18
Console(config-if)#spanning-tree protocol-migration             31-24
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Multiple Spanning Trees

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 65 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 12-11) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (STA Configuration, page 12-8).
2. Enter the spanning tree priority for the selected MST instance (MSTP VLAN Configuration).
3. Add the VLANs that will share this MSTI (MSTP VLAN Configuration).

Note: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

Command Attributes

- **MST Instance** – Instance identifier of this spanning tree. (Default: 0)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

Downloaded from www.Manualslib.com manuals search engine

- **VLANs in MST Instance** – VLANs assigned this instance.
- **MST ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **VLAN ID** – VLAN to assign to this selected MST instance. (Range: 1-4093)

The other global attributes are described under "Displaying Global Settings," page 12-4. The attributes displayed by the CLI for individual interfaces are described under "Displaying Interface Settings," page 12-13

Web – Click Spanning Tree, MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.

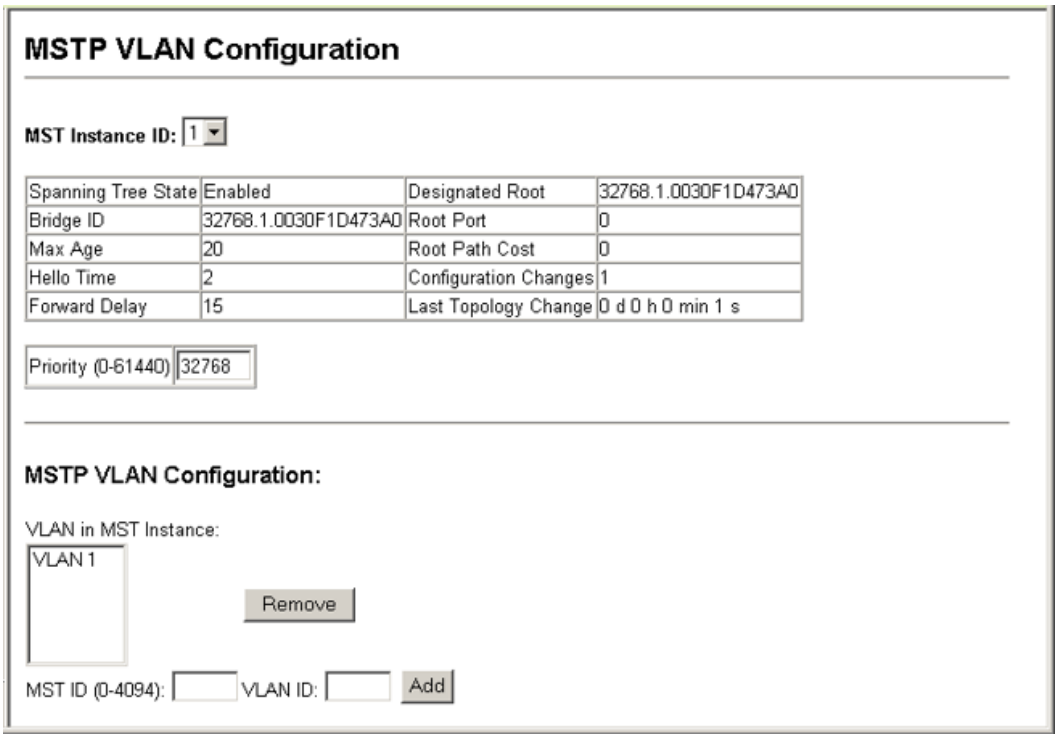


Figure 12-5 MSTP VLAN Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This displays STA settings for instance 1, followed by settings for each port.

```
Console#show spanning-tree mst 1                                    31-25
Spanning-tree information
---------------------------------------------------------------------
 Spanning Tree Mode:               MSTP
 Spanning Tree Enabled/Disabled:   Enabled
 Instance:                         1
 VLANs Configuration:              1
 Priority:                         32768
 Bridge Hello Time (sec.):         2
 Bridge Max Age (sec.):            20
 Bridge Forward Delay (sec.):      15
 Root Hello Time (sec.):           2
 Root Max Age (sec.):              20
 Root Forward Delay (sec.):        15
 Max Hops:                         20
 Remaining Hops:                   20
 Designated Root:                  32768.1.000000001111
 Current Root Port:                7
 Current Root Cost:                10000
 Number of Topology Changes:       1
 Last Topology Change Time (sec.): 14
 Transmission Limit:               3
 Path Cost Method:                 Long

---------------------------------------------------------------------
Eth  1/ 7 information
---------------------------------------------------------------------
 Admin Status:             Enabled
 Role:                     Master
 State:                    Forwarding
 External admin path cost: 10000
 Internal admin path cost: 10000
 External oper path cost:  10000
 Internal oper path cost:  10000
 Priority:                 128
 Designated cost:          0
 Designated port:          128.1
 Designated root:          32768.1.0030F1D473A0
 Designated bridge:        32768.1.0030F1D473A0
 Fast forwarding:          Disabled
 Forward transitions:      1
 Admin edge port:          Disabled
 Oper edge port:           Disabled
 Admin Link type:          Auto
 Oper Link type:           Point-to-point
 Spanning Tree Status:     Enabled
:
```


Downloaded from www.Manualslib.com manuals search engine

CLI – This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

```
Console(config)#spanning-tree mst-configuration                    31-10
Console(config-mst)#mst 1 priority 4096                            31-12
Console(config-mstp)#mst 1 vlan 1-5                                31-11
Console(config-mst)#
```

Displaying Interface Settings for MSTP

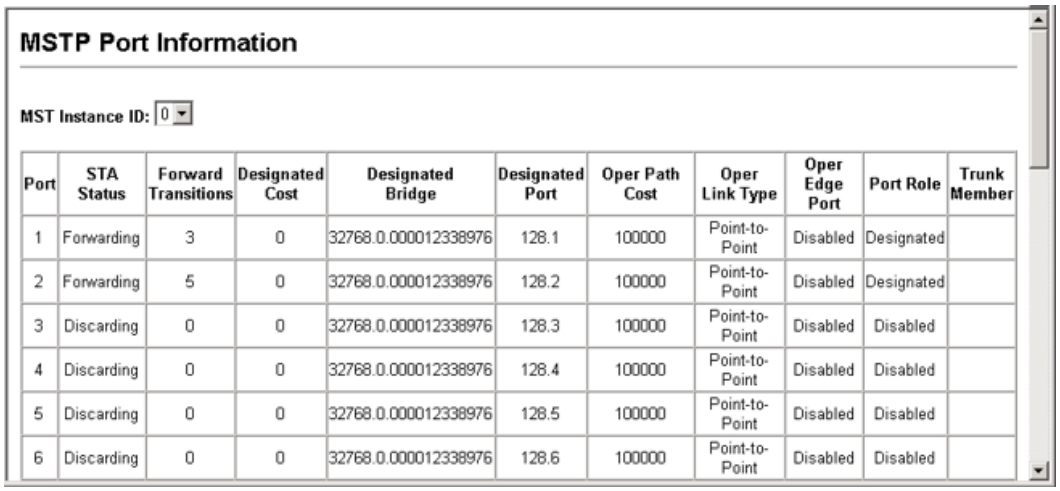
The MSTP Port Information and MSTP Trunk Information pages display the current status of ports and trunks in the selected MST instance.

Field Attributes

MST Instance ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

Note: The other attributes are described under "Displaying Interface Settings," page 12-13.

Web – Click Spanning Tree, MSTP, Port Information or Trunk Information. Select the required MST instance to display the current spanning tree values.



MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	3	0	32768.0.000012338976	128.1	100000	Point-to-Point	Disabled	Designated	
2	Forwarding	5	0	32768.0.000012338976	128.2	100000	Point-to-Point	Disabled	Designated	
3	Discarding	0	0	32768.0.000012338976	128.3	100000	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0.000012338976	128.4	100000	Point-to-Point	Disabled	Disabled	
5	Discarding	0	0	32768.0.000012338976	128.5	100000	Point-to-Point	Disabled	Disabled	
6	Discarding	0	0	32768.0.000012338976	128.6	100000	Point-to-Point	Disabled	Disabled	

Figure 12-6 MSTP Port Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This displays STA settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the IST (page 12-4), the settings for other instances only apply to the local spanning tree.

```
Console#show spanning-tree mst 0                                    31-25
Spanning-tree information
---------------------------------------------------------------------
 Spanning Tree Mode:                MSTP
 Spanning Tree Enabled/Disabled:    Enabled
 Instance:                          0
 VLANs Configuration:               2-4094
 Priority:                          32768
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Max Hops:                          20
 Remaining Hops:                    20
 Designated Root:                   32768.0.000000001111
 Current Root Port:                 1
 Current Root Cost:                 10000
 Number of Topology Changes:        12
 Last Topology Change Time (sec.): 303

 Transmission Limit:                3
 Path Cost Method:                  long
---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
 Admin Status:              Enabled
 Role:                      Root
 State:                     Forwarding
 External Admin Path Cost: 100000
 Internal Admin Path Cost: 100000
 External Oper Path Cost:  100000
 Internal Oper Path Cost:  100000
 Priority:                  128
 Designated Cost:           0
 Designated Port:           128.4
 Designated Root:           32768.0.0000E8AAAA00
 Designated Bridge:         32768.0.0000E8AAAA00
 Fast Forwarding:           Disabled
 Forward Transitions:       2
 Admin Edge Port:           Disabled
 Oper Edge Port:            Disabled
 Admin Link Type:           Auto
 Oper Link Type:            Point-to-point
 Spanning Tree Status:      Enabled
:
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Interface Settings for MSTP

You can configure the STA interface settings for an MST Instance using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 12-13 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16

Downloaded from www.Manualslib.com manuals search engine

- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) (Range: 0 for auto-configuration, 1-65535 for the short path cost method[17], 1-200,000,000 for the long path cost method)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

  The recommended range is listed in Table 12-1 on page 12-19.
  The recommended path cost is listed in Table 12-2 on page 12-19.
  Default path costs use the IEEE 802.1w-2001 recommendations listed in Table 12-2 on page 12-19, except when short path cost method is selected and the recommended value would fall below 65,535 (i.e., the minimum default setting).

17. Refer to "Configuring Global Settings" on page 12-8 for information on setting the path cost method.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Spanning Tree, MSTP, Port Configuration or Trunk Configuration. Enter the priority and path cost for an interface, and click Apply.

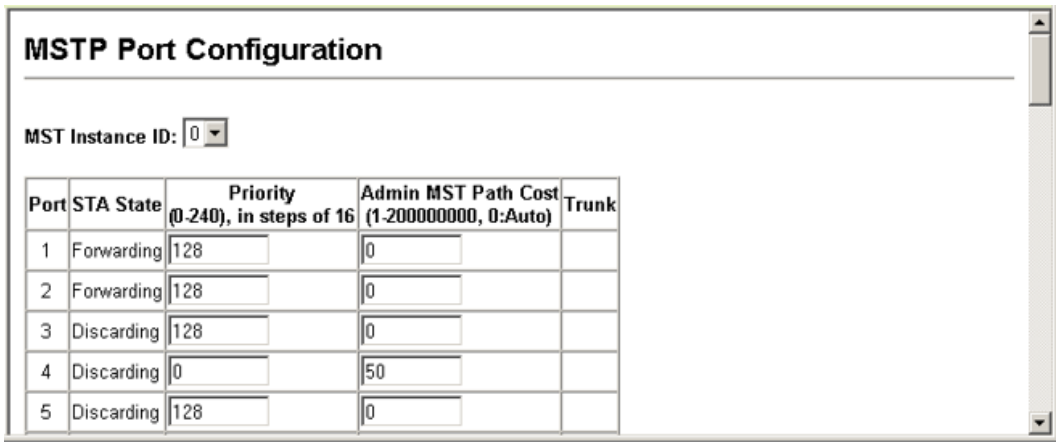


Figure 12-7 MSTP Port Configuration

CLI – This example sets the MSTP attributes for port 4.

```
Console(config)#interface ethernet 1/4                    25-2
Console(config-if)#spanning-tree mst port-priority 0      31-23
Console(config-if)#spanning-tree mst cost 50              31-22
Console(config-if)
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 13
VLAN CONFIGURATION

Selecting the VLAN Operation Mode

The system can be configured to operate in normal mode or one of the tunneling modes used for passing Layer 2 traffic across a service provider's metropolitan area network, including IEEE 802.1Q tunneling (QinQ) or static VLAN tag swapping (VLAN Swap).

Command Attributes

- **Normal** – The switch functions in normal operating mode.
  This is the default operating mode, and should be placed in this mode when using standard IEEE 802.1Q VLANs (page 13-2), private VLANs (page 13-18), or protocol VLANs (page 13-20).
- **QinQ** – Sets the switch to QinQ mode, and allows the QinQ tunnel port to be configured. For an explanation of QinQ, see "Configuring IEEE 802.1Q Tunneling" on page 13-24.
- **VLAN Swap** – Sets the switch to VLAN Swap mode, which swaps VLAN tags when packets are passed between the service provider and customer. For an explanation of VLAN swapping, see "Configuring VLAN Swapping" on page 13-33.

Note: If there are any dot1q-tunnel ports set on the switch, the system will not be able to exit QinQ mode (see "Configuring IEEE 802.1Q Tunneling" on page 13-24).

Downloaded from www.Manualslib.com manuals search engine

Web – Click VLAN, System Mode. Select the required mode, click Apply.

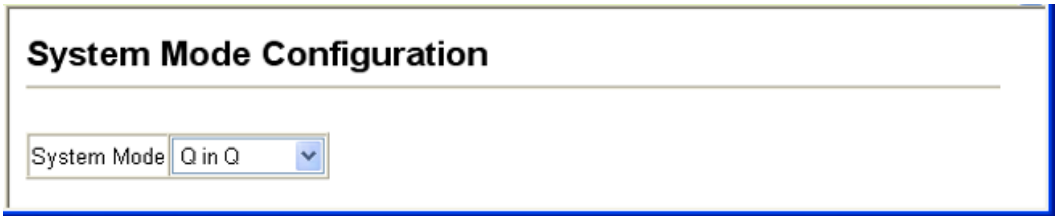


Figure 13-1 Selecting the System Mode

CLI – This example sets the switch to operate in QinQ mode.

```
Console(config)#system mode qinq                                    20-13
Console(config)#
```

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

Downloaded from www.Manualslib.com manuals search engine

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

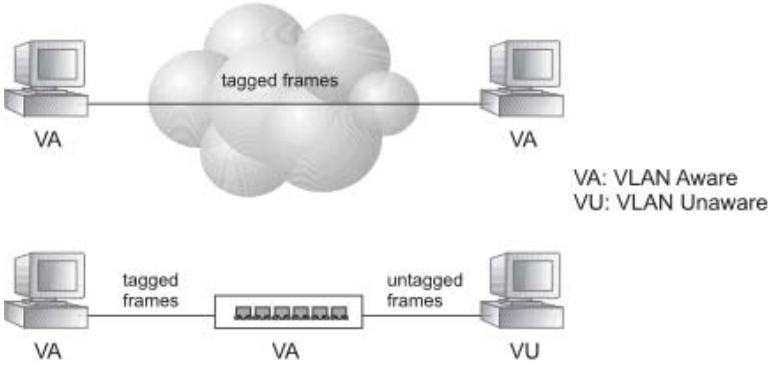
- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

Downloaded from www.Manualslib.com manuals search engine



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

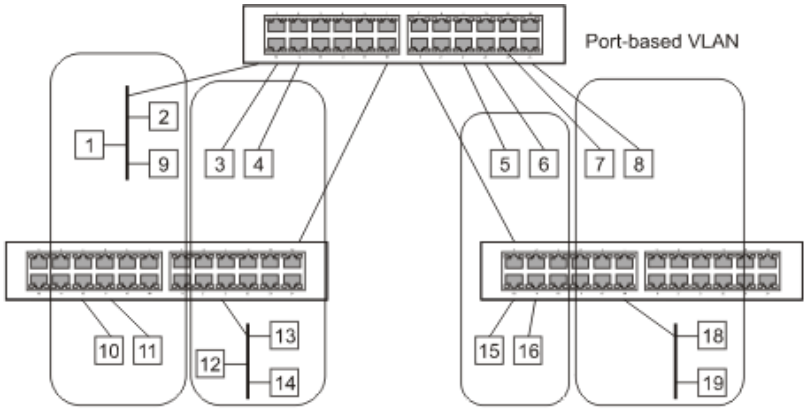
Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then

Downloaded from www.Manualslib.com manuals search engine

forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs (VLAN Index)" on page 13-12). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several

Downloaded from www.Manualslib.com manuals search engine

switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Enabling or Disabling GVRP (Global Setting)

ARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.
(Default: Disabled)

Web – Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, click Apply

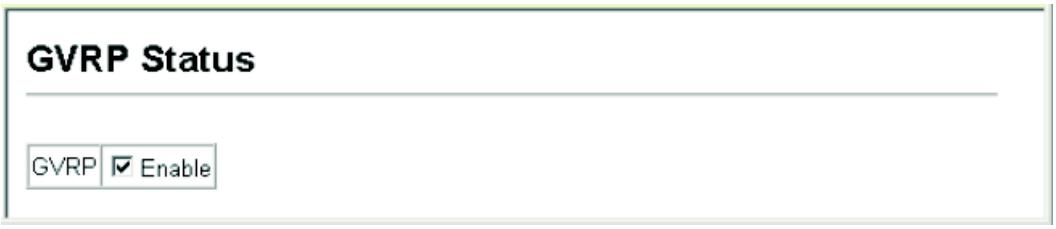


Figure 13-2 Globally Enabling GVRP

Downloaded from www.Manualslib.com manuals search engine

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp                                    32-2
Console(config)#
```

Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

- **VLAN Version Number**[18] – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

Web – Click VLAN, 802.1Q VLAN, Basic Information.

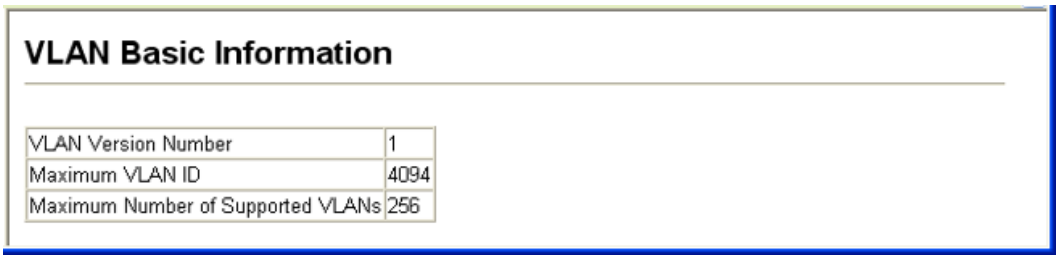


Figure 13-3 VLAN Basic Information

18. Web Only.

Downloaded from www.Manualslib.com manuals search engine

CLI – Enter the following command.

```
Console#show bridge-ext                                          32-3
 Max Support VLAN Numbers:              255
 Max Support VLAN ID:                   4094
 Extended Multicast Filtering Services: No
 Static Entry Individual Port:          Yes
 VLAN Learning:                         IVL
 Configurable PVID Tagging:             Yes
 Local VLAN Capable:                    No
 Traffic Classes:                       Enabled
 Global GVRP Status:                    Disabled
 GMRP:                                  Disabled
Console#
```

Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Downloaded from www.Manualslib.com manuals search engine

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.

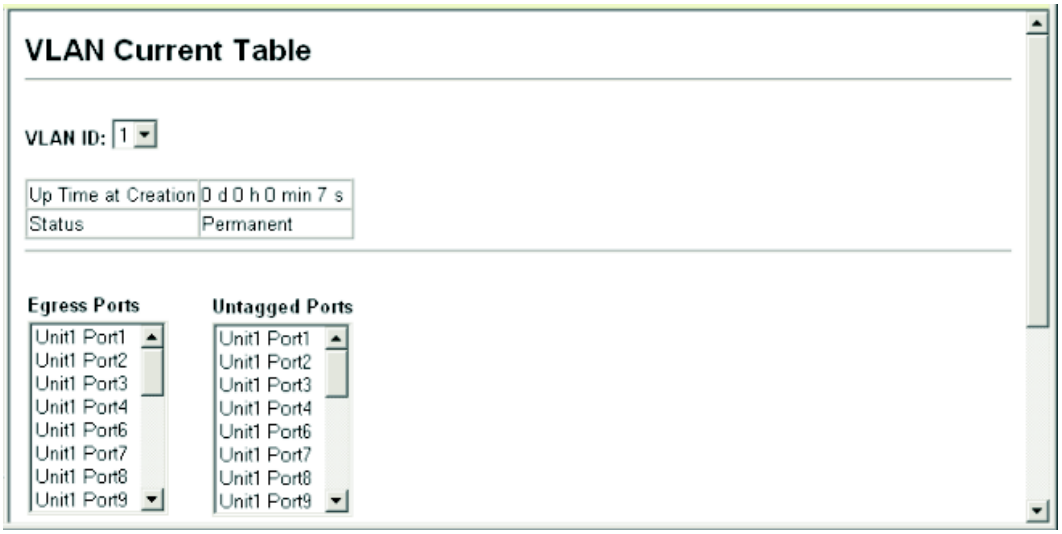


Figure 13-4 VLAN Current Table

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

Downloaded from www.Manualslib.com manuals search engine

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                          32-16

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S)
Console#
```

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status** (Web) – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **State** (CLI) – Enables or disables the specified VLAN.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.

Downloaded from www.Manualslib.com manuals search engine

- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

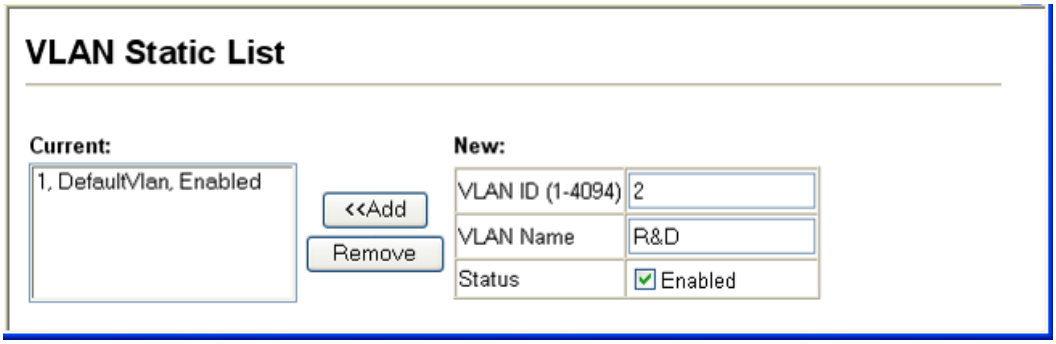


Figure 13-5 VLAN Static List - Creating VLANs

CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                          32-7
Console(config-vlan)#vlan 2 name R&D media ethernet state active       32-8
Console(config-vlan)#end
Console#show vlan                                                      32-16

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S)
.
.
.
VLAN ID:               2
Type:                  Static
Name:                  R&D
Status:                Active
Ports/Port Channels:

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

Notes: **1.** You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 13-14). However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under "Configuring VLAN Behavior for Interfaces" on page 13-15.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.

Downloaded from www.Manualslib.com manuals search engine

  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see "Automatic VLAN Registration" on page 13-4.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.

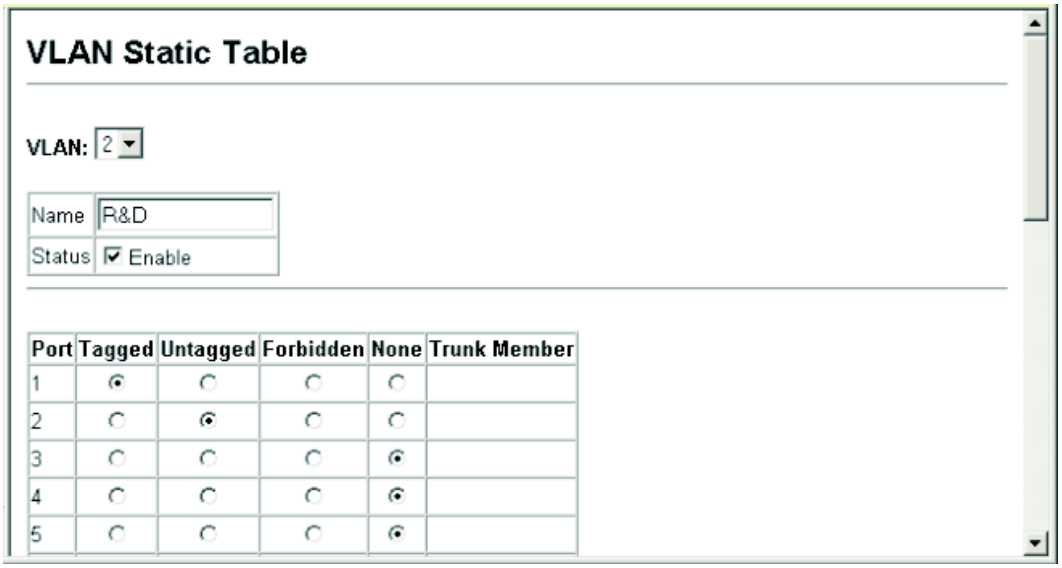


Figure 13-6 VLAN Static Table - Adding Static Members

CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config-if)#switchport allowed vlan add 2 tagged         32-14
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, 802.1Q VLAN, Static Membership by Port. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.

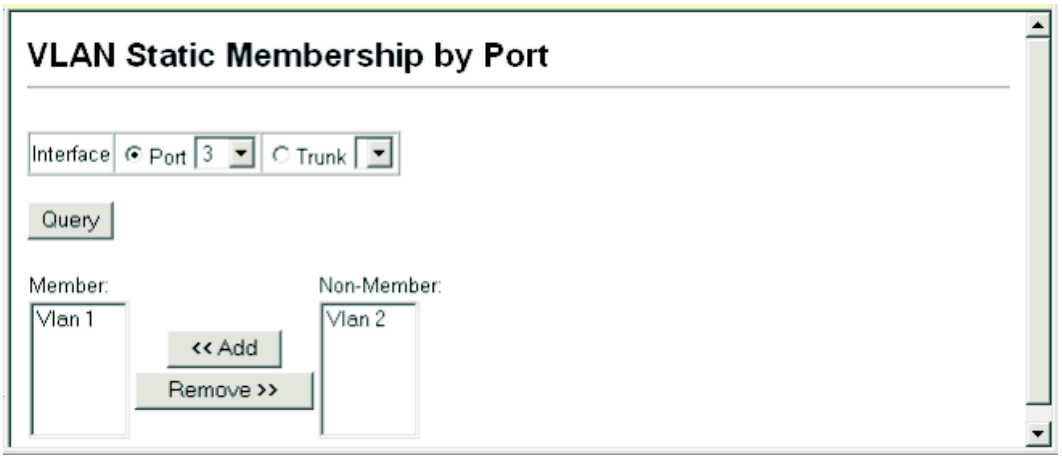


Figure 13-7 VLAN Static Membership by Port

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                          25-2
Console(config-if)#switchport allowed vlan add 1 tagged         32-14
Console(config-if)#switchport allowed vlan remove 2
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/ deregistration.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
  - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
  - Ingress filtering only affects tagged frames.

Downloaded from www.Manualslib.com manuals search engine

- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See "Displaying Bridge Extension Capabilities" on page 4-9.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)
- **GARP Join Timer**[19] – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave Timer**[19] – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer**[19] – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)
- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames

19. Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

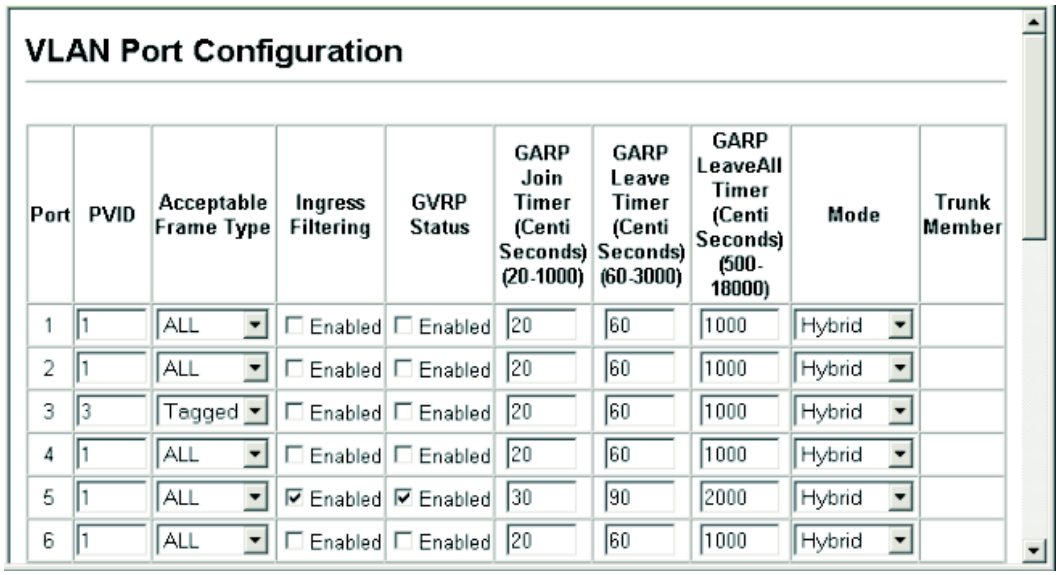
Downloaded from www.Manualslib.com manuals search engine

belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

- **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration. Fill in the required settings for each interface, click Apply.



VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
2	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
3	3	Tagged	Enabled	Enabled	20	60	1000	Hybrid	
4	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	
5	1	ALL	Enabled	Enabled	30	90	2000	Hybrid	
6	1	ALL	Enabled	Enabled	20	60	1000	Hybrid	

Figure 13-8 VLAN Port Configuration

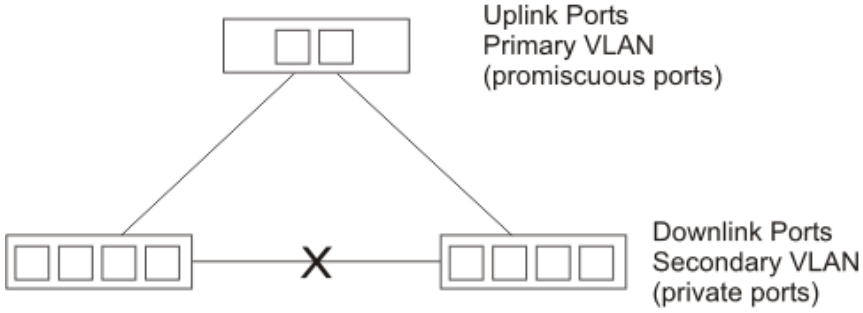
CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3                          25-2
Console(config-if)#switchport acceptable-frame-types tagged     32-11
Console(config-if)#switchport ingress-filtering                 32-12
Console(config-if)#switchport native vlan 3                     32-13
Console(config-if)#switchport gvrp                              32-4
Console(config-if)#garp timer join 20                           32-5
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid                       32-10
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click VLAN, Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.

Figure 13-9 Private VLAN Status

CLI – This example enables private VLANs.

```
Console(config)#pvlan                                    32-17
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Web – Click VLAN, Private VLAN, Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.

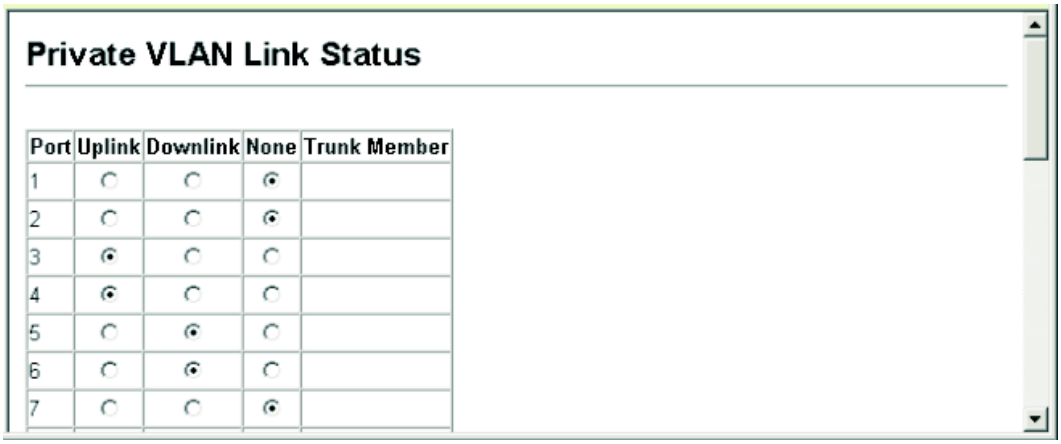


Figure 13-10 Private VLAN Link Status

CLI – This configures port 3 as an uplink and port 5 and 6 as downlinks.

```
Console(config)#pvlan up-link ethernet 1/3 down-link ethernet 1/5
32-17
Console(config)#pvlan up-link ethernet 1/3 down-link ethernet 1/6
Console(config)#end
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/3
Down-link port:
 Ethernet 1/5
 Ethernet 1/6
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Protocol-Based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 13-10). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.
3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

Downloaded from www.Manualslib.com manuals search engine

Configuring Protocol Groups

Create a protocol group for one or more protocols.

Command Attributes

- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **Frame Type**[20] – Frame type used by this protocol. (Options: Ethernet, RFC_1042, LLC_other)
- **Protocol Type** – The only option for the LLC_other frame type is IPX_raw. The options for all other frames types include: IP, ARP, and RARP.

Web – Click VLAN, Protocol VLAN, Configuration. Enter a protocol group ID, frame type and protocol type, then click Apply.

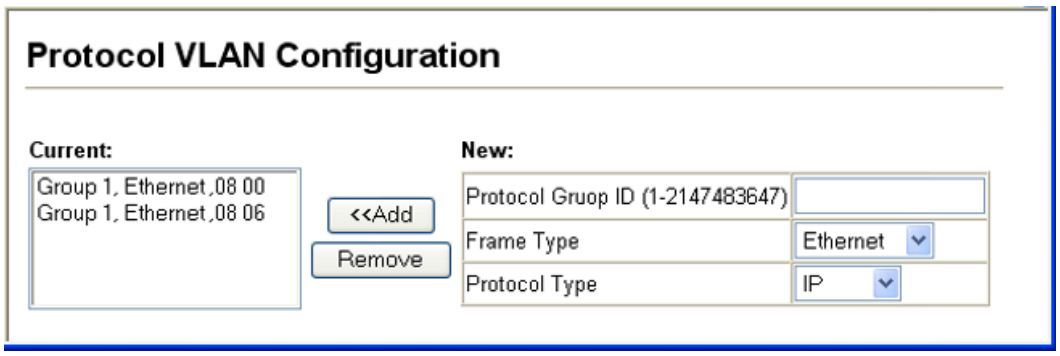


Figure 13-11 Protocol VLAN Configuration

CLI – The following creates protocol group 1, and then specifies Ethernet frames with IP and ARP protocol types.

```
Console(config)#protocol-vlan protocol-group 1
  add frame-type ethernet protocol-type ip                    32-21
Console(config)#protocol-vlan protocol-group 1
  add frame-type ethernet protocol-type arp
Console(config)#
```

20. SNAP frame types are not supported by this switch due to hardware limitations.

Downloaded from www.Manualslib.com manuals search engine

Mapping Protocols to VLANs

Map a protocol group to a VLAN for each interface that will participate in the group.

Command Usage

- When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN menus such as the VLAN Static Table (page 13-12) or VLAN Static Membership by Port menu (page 13-14), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

Downloaded from www.Manualslib.com manuals search engine

Web – Click VLAN, Protocol VLAN, Port Configuration. Select a a port or trunk, enter a protocol group ID, the corresponding VLAN ID, and click Apply.

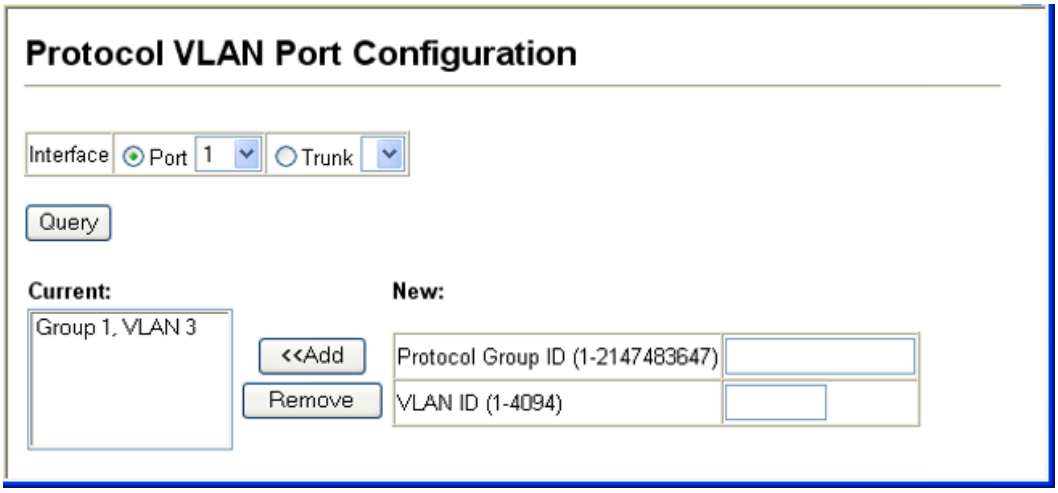


Figure 13-12 Protocol VLAN Port Configuration

CLI – The following maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2      32-22
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IEEE 802.1Q Tunneling

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

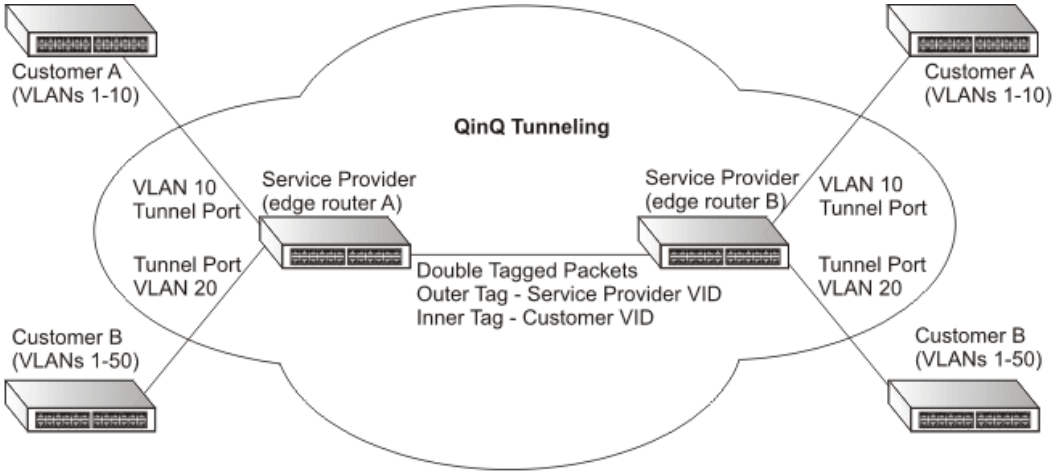
A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate SPVLAN, but this VLAN will support all of the customer's internal VLANs. The QinQ uplink port that passes traffic from the edge switch into the service provider's metro network must also

Downloaded from www.Manualslib.com manuals search engine

be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.



Layer 2 Flow for Packets Coming into a Tunnel Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

Downloaded from www.Manualslib.com manuals search engine

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. New SPVLAN tags are added to all incoming packets, no matter how many tags they already have. The ingress process constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag). This outer tag is used for learning and switching packets. The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet (and this feature is enabled on the switch).
2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.
3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).
4. The switch sends the packet to the proper egress port.
5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into an Uplink Port

An uplink port receives one of the following packets:

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

Downloaded from www.Manualslib.com manuals search engine

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.
3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookup, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.
5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The switch sends the packet to the proper egress port.

Downloaded from www.Manualslib.com manuals search engine

8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

- The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes none-customer packets to be forwarded to SPVLAN.
- Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.
- QinQ and VLAN Swap mode cannot be supported at the same time.
- The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, VLAN 1 can be used as a management VLAN instead of a data VLAN in the service provider network.
- There are some inherent incompatibilities between Layer 2 and Layer 3 features when using 802.1Q tunneling:
  - Tunnel ports do not support IP Access Control Lists.
  - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
  - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (see "Selecting the VLAN Operation Mode" on page 13-1).
2. Create a Service Provider VLAN, also referred to as an SPVLAN (see "Creating VLANs" on page 13-10).
3. Configure the QinQ tunnel port to dot1Q tunnel port mode (see "Adding an Interface to a QinQ Tunnel" on page 13-30).

Downloaded from www.Manualslib.com manuals search engine

4. Set the Tag Protocol Identifier (TPID) value of the tunnel port. This step is required is the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See "Adding an Interface to a QinQ Tunnel" on page 13-30.)
5. Configure the QinQ tunnel port to join the SPVLAN as an untagged member (see "Adding Static Members to VLANs (VLAN Index)" on page 13-12).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel port (see "Configuring VLAN Behavior for Interfaces" on page 13-15).
7. Configure the QinQ uplink port to join the SPVLAN as a tagged member (see "Adding Static Members to VLANs (VLAN Index)" on page 13-12).

Downloaded from www.Manualslib.com manuals search engine

Adding an Interface to a QinQ Tunnel

Follow the guidelines in the preceding section to set up a QinQ tunnel on the switch. Set the ingress port on the service provider's network to dot1Q tunnel mode. Set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. And specify whether or not to copy the priority bits from the inner VLAN tag to the outer VLAN tag.

Command Attributes

- **Switchport Mode** – Set the VLAN membership mode dot1Q-Tunnel.
- **Dot1q-Ethertype TPID** – The Tag Protocol Identifier specifies the ethertype of incoming packets on a tunnel port. (Range: 0-65535; Default: not set)

  Use the TPID field to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

  All members of a VLAN should be set to the same ethertype.
- **QinQ Priority Map** – Copies the priority bits from the inner VLAN tag used by customer to the outer VLAN tag used by service provider. (Default: Disabled)

  The packet must have a standard ethertype value of 0x8100 for this command to take effect. Otherwise, the priority bits in the outer tag are set to zero.

  Using a fixed priority level for all customer traffic allows the service provider to more easily calculate the resources required to maintain adequate bandwidth for a large number of customers. However, if it is

Downloaded from www.Manualslib.com manuals search engine

necessary to support real-time services across the backbone network, then you may have to enable priority bit mapping from the inner to outer VLAN tag to ensure timely service.

Web – Click VLAN, 802.1 Q Tunneling. Set the mode for the tunnel port to Dot1q-Tunnel, set the TPID if the client is using a non-standard ethertype to identify 802.1Q tagged frames, and specify whether or not to copy the priority bits from the inner VLAN tag to the outer tag. Then click Apply.

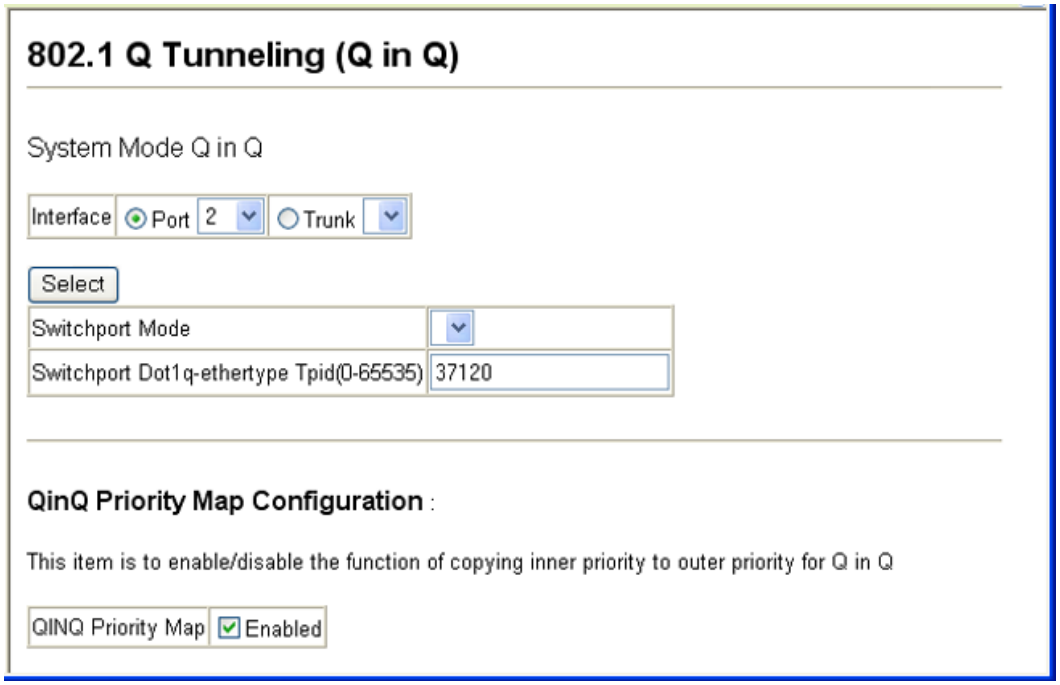


Figure 13-13 Tunnel Port Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This example configures the switch to copy the priority bits from the inner to outer VLAN tag, it then sets port 2 to tunnel mode, and indicates that the TPID used for 802.1Q tagged frames will be 9100 hexadecimal.

```
Console(config)#qinq priority map                                  32-26
Console(config)#interface ethernet 1/2                             25-2
Console(config-if)#switchport mode dot1q-tunnel                    32-27
Console(config-if)#switchport dot1q-ethertype 9100                 32-29
Console(config-if)#exit
Console#show dot1q-tunnel                                          32-28
dot1q tunnel port:
ethernet
1/2
port channel

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring VLAN Swapping

QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the local switches connected directly to the customer can be manually configured to swap the customer's VLAN ID with the service provider's VLAN ID.

General Configuration Guidelines for VLAN Swapping

1. Configure the switch to VLAN-swap mode (see "Selecting the VLAN Operation Mode" on page 13-1).
2. For traffic entering the switch through a downlink port attached to a customer (i.e., inbound port and VLAN) and exiting through an uplink port attached to a service provider (i.e., outbound port and VLAN), map the inbound to outbound port, and inbound to outbound VLAN.
3. For traffic entering the switch through an uplink port attached to a service provider (i.e., inbound port and VLAN) and exiting through an downlink port (i.e., outbound port and VLAN), map the inbound to outbound port, and inbound to outbound VLAN.

Command Usage

- VLAN swapping only supports one-to-one mapping of VLAN IDs between a VDSL port and an uplink port.
- VLAN IDs must be mapped for both the upstream and downstream direction.
- The maximum number of VLAN swap entries is 64 per port groups 1-8, 9-16, 17, and 18. However, note that configuring a large number of entries may degrade the performance of other processes that also use the Fast Forwarding Processor (FFP) table, such as access lists, rate limiting, and IP filtering.

Downloaded from www.Manualslib.com manuals search engine

Field Attributes

- **Entry Counts** – The number of entries in the VLAN swapping table.
- **VLAN Swap Table** – Contains each entry in the VLAN swapping table.
- **InPort** – Port through which traffic is entering the switch. (Range: 1-18)
- **OutPort** – Port through which traffic is leaving the switch. (Range: 1-18)
- **InVLAN** – VLAN associated with the InPort. (Range: 1-4093)
- **OutVLAN** – VLAN associated with the OutPort. (Range: 1-4093)

Web – Click VLAN, VLAN Swap. Select the port and VLAN through which traffic is entering the switch, set the corresponding port and VLAN through which traffic is leaving the switch, and click Add VLAN Swap.

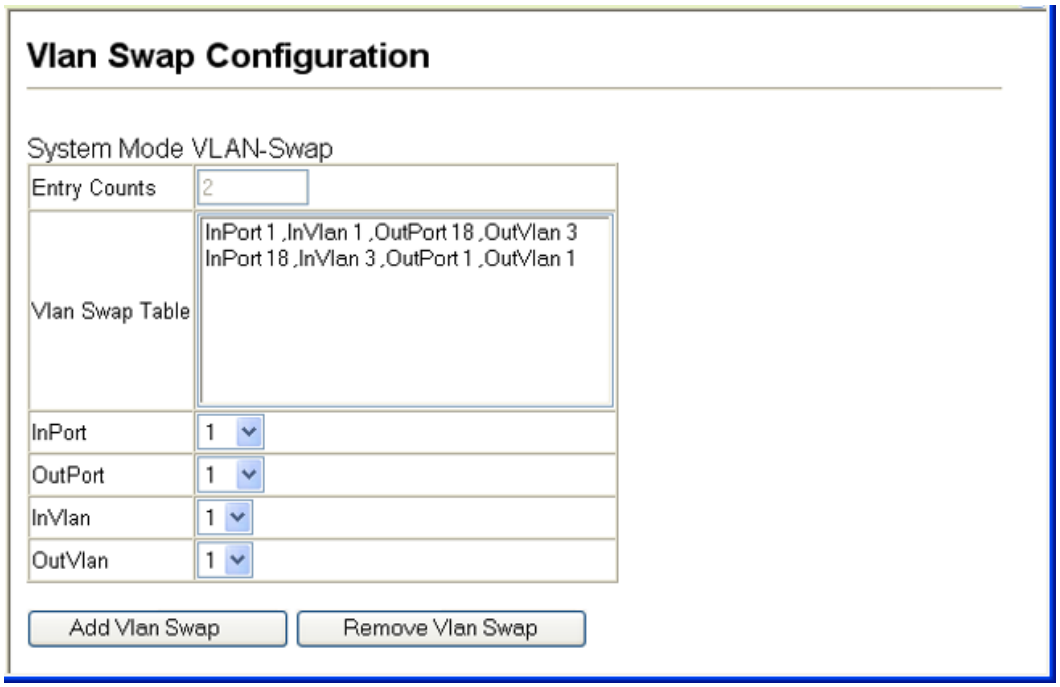


Figure 13-14 VLAN Swap Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This example configures VLAN swapping for upstream traffic between port 1 and port 18, exchanging VLAN ID 1 for VLAN ID 3. It then sets VLAN swapping for downstream traffic to exchange VLAN ID 3 for VLAN ID 1.

```
Console(config)#system mode vlan-swap                          20-13
Console(config)#interface ethernet 1/1                         25-2
Console(config-if)#switchport vlan swap 1 3 1/18               32-27
Console(config-if)#exit
Console(config)#interface ethernet 1/18
Console(config-if)#switchport vlan swap 3 1 1/1
Console(config-if)#end
Console#show vlan swap
vlan-swap enable
ethernet 1/1
    invlan    outvlan    outport
    1         3          1/18
ethernet 1/18
    invlan    outvlan    outport
    3         1          1/1
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 14
CLASS OF SERVICE

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Layer 2 Queue Settings

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **Default Priority**[21] – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.

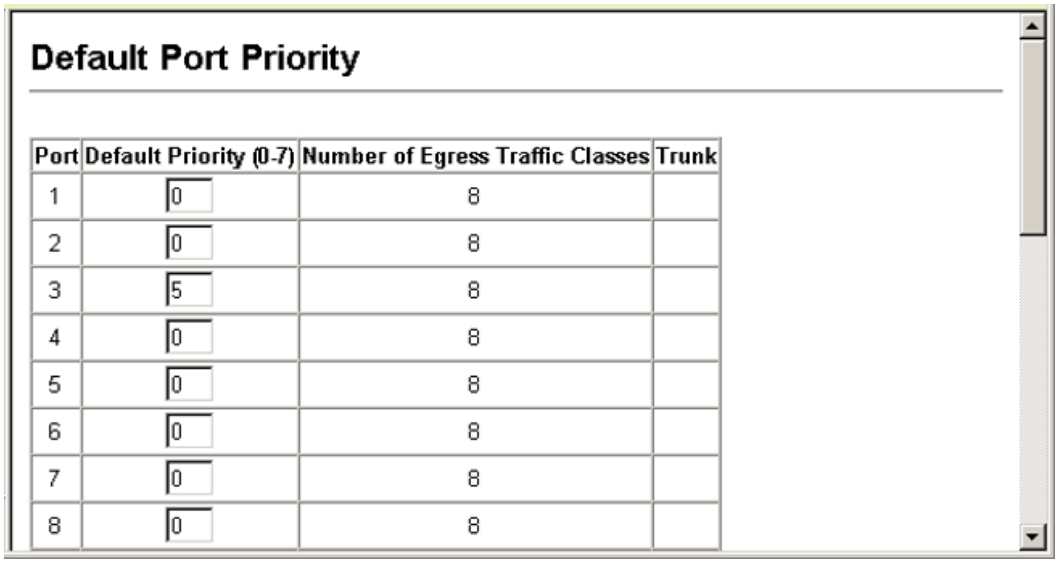


Figure 14-1 Default Port Priority

21. CLI displays this information as "Priority for untagged traffic."

Downloaded from www.Manualslib.com manuals search engine

CLI – This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3                          25-2
Console(config-if)#switchport priority default 5                33-17
Console(config-if)#end
Console#show interfaces switchport ethernet 1/3                 25-16
Information of Eth 1/3
 Broadcast Threshold:            Enabled, 500 packets/second
 Multicast Threshold:            Enabled, 500 packets/second
 Unknown Unicast Threshold:      Enabled, 500 packets/second
 LACP Status:                    Disabled
 Ingress Rate Limit:             Disabled, 102400K bits per second
 Egress Rate Limit:              Disabled, 102400K bits per second
 Ingress Rate Limit Trap:        Disabled, Up:0 packets,Down:0 packets
 VLAN Membership Mode:           Hybrid
 Ingress Rule:                   Disabled
 Acceptable Frame Type:          All frames
 Native VLAN:                    1
 Priority for Untagged Traffic: 0
 GVRP Status:                    Disabled
 MDIX Status:                    Auto
 Allowed VLAN:                      1(u),
 Forbidden VLAN:
Console#
```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 14-1 Mapping CoS Values to Egress Queues

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

Downloaded from www.Manualslib.com manuals search engine

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Table 14-2 CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class**[22] – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

22. CLI shows Queue ID.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Priority, Traffic Classes. Assign priorities to the traffic classes (i.e., output queues), then click Apply.

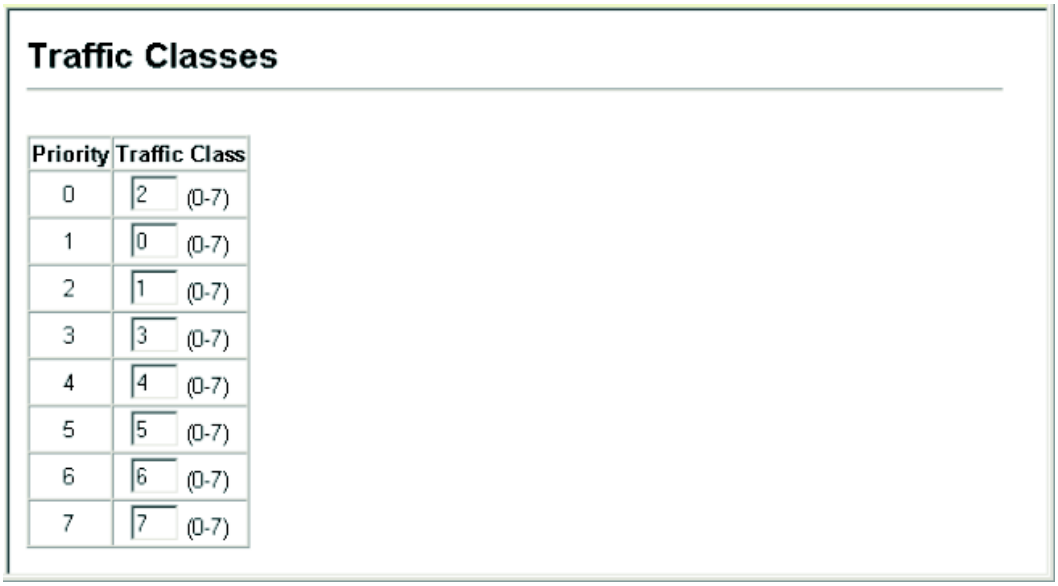


Figure 14-2 Traffic Classes

CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config)#queue cos-map 0 0                               33-8
Console(config)#queue cos-map 1 1
Console(config)#queue cos-map 2 2
Console(config)#exit
Console#show queue cos-map                                      33-10
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Information of Eth 1/2
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
⋮
```

* Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue, or a combination of strict service for the high priority queues and weighted queueing for the remaining queues.

Command Usage

- The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queueing.
- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- WRR specifies a relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.
- Hybrid mode uses strict priority on the high-priority queues and WRR on the rest of the queues.

Command Attributes

- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **WRR** - Weighted Round-Robin shares bandwidth at the egress ports by using the default scheduling weights of 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively. (This is the default selection.)
- **Hybrid** - Strict priority is used for the high-priority queues and Weighted Round-Robin for the rest of the queues. The high priority queues are specified by setting a queue's bandwidth to zero (see "Setting the Service Weight for Traffic Classes" on page 14-7).

Downloaded from www.Manualslib.com manuals search engine

Web – Click Priority, Queue Mode. Select Strict or WRR, then click Apply.

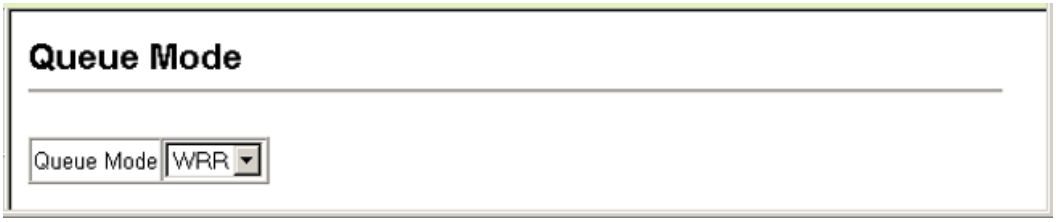


Figure 14-3 Queue Mode

CLI – The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict                              33-2
Console(config)#exit
Console#show queue mode                                        33-2

Queue mode: strict
Console#
```

Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in "Mapping CoS Values to Egress Queues" on page 14-3, the traffic classes are mapped to one of the eight egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Usage

- WRR controls bandwidth sharing at the egress port by defining scheduling weights for allocated service priorities. When using WRR, assign a weight of 1-15 to each of the hardware queues.
- Hybrid mode uses strict priority processing on the high-priority queues, and WRR on the remaining queues. When using hybrid mode, assign a weight of zero to indicate a high-priority queue. Any of queues 2 - 7 can be specified as high-priority queues, but the selected queues must be in consecutive order, and must all be grouped toward the high end of the queue list as shown in the following example.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **WRR Setting Table**[23] – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Set a new weight for the selected traffic class. (Range: 0-15)

  Use queue weights 1-15 for queues allocated service time based on WRR. Queue weights must be configured in ascendant manner, assigning more weight to each higher numbered queue. Use queue weight zero to indicate a high-priority queue (processed first based on strict priority) when using the hybrid queue mode.

Web – Click Priority, Queue Scheduling. Select the interface, highlight a traffic class (i.e., output queue), enter a weight, then click Apply.

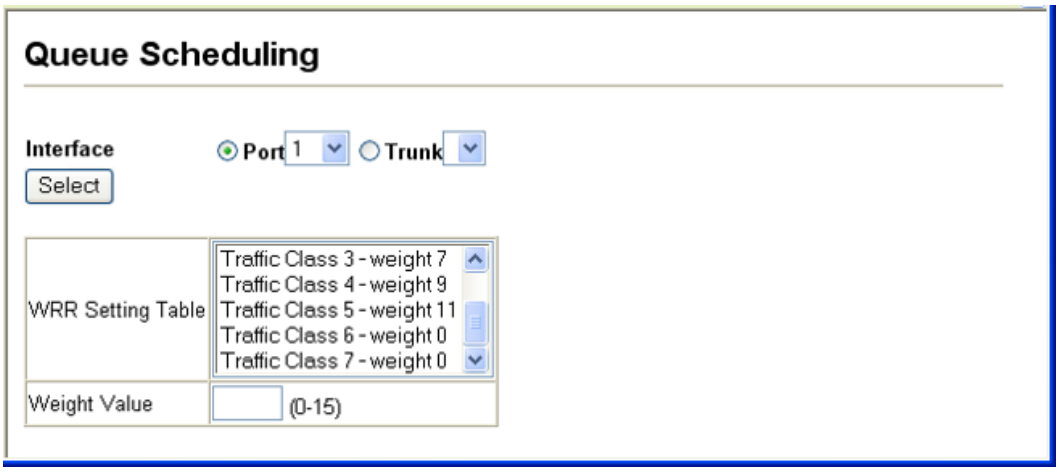


Figure 14-4 Queue Scheduling

23. CLI shows Queue ID.

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example shows how to assign WRR weights to priority queues 0-5, and strict priority to queues 6 and 7.

```
Console(config)#interface ethernet 1/1                          25-2
Console(config-if)#queue bandwidth 1 3 5 7 9 11 0 0             33-7
Console(config-if)#end
Console#show queue bandwidth                                    33-9
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0        1
    1        3
    2        5
    3        7
    4        9
    5        11
    6        0
    7        0
Information of Eth 1/2
 Queue ID  Weight
⋮
```

Layer 3/4 Priority Settings

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

Downloaded from www.Manualslib.com manuals search engine

Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu, then click Apply.

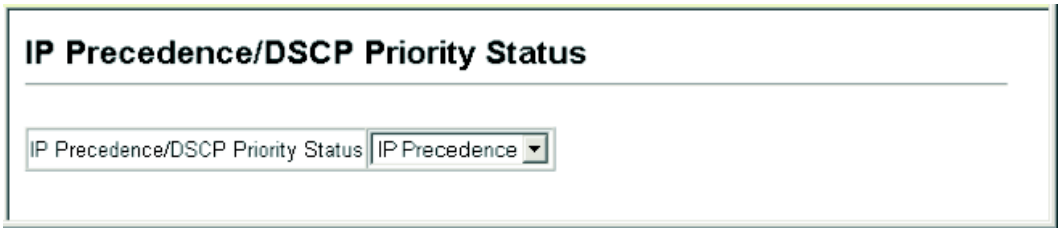


Figure 14-5 IP Precedence/DSCP Priority Status

CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                              33-13
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Table 14-3 Mapping IP Precedence

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precedence value. Note that "0" represents low priority and "7" represent high priority.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Priority, IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.

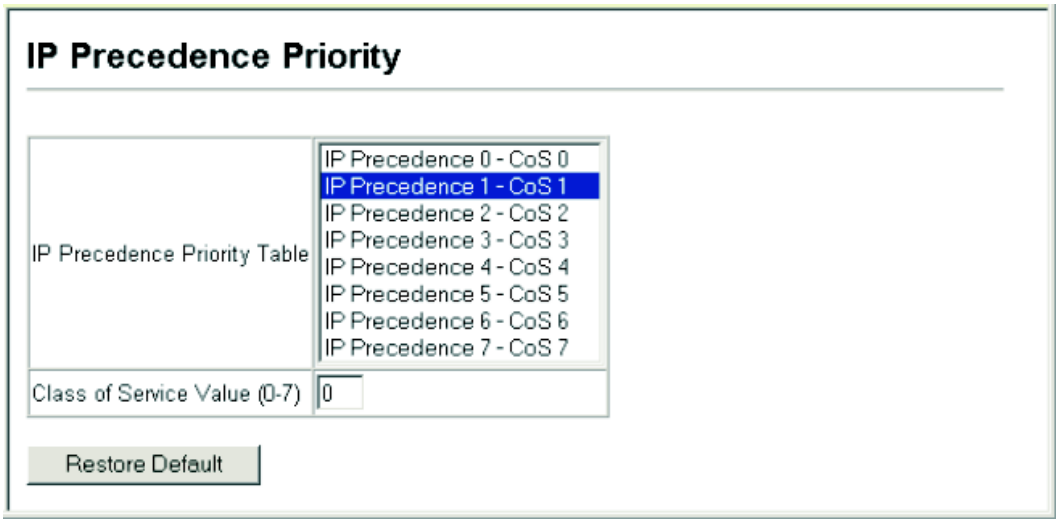

IP Precedence Priority
IP Precedence Priority Table
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7
Class of Service Value (0-7)
0
Restore Default

Figure 14-6 IP Precedence Priority

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```
Console(config)#map ip precedence                              33-13
Console(config)#interface ethernet 1/1                         25-2
Console(config-if)#map ip precedence 1 cos 0                   33-14
Console(config-if)#end
Console#show map ip precedence ethernet 1/1                    33-19
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 14-4 Mapping DSCP Priority

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that "0" represents low priority and "7" represent high priority.

Note: IP DSCP settings apply to all interfaces.

Downloaded from www.Manualslib.com manuals search engine

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.

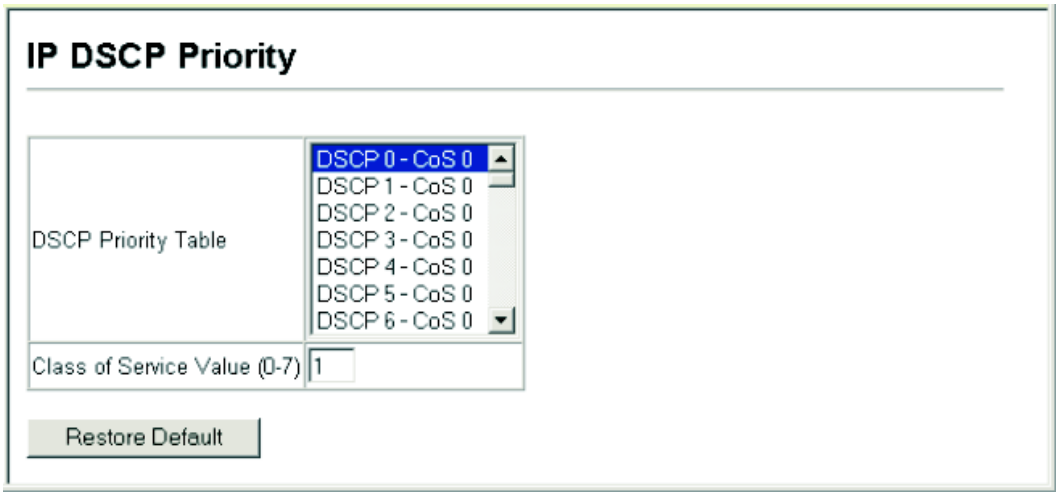

IP DSCP Priority
DSCP Priority Table
DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
Class of Service Value (0-7)
1
Restore Default

Figure 14-7 IP DSCP Priority

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp                                    33-15
Console(config)#interface ethernet 1/1                         25-2
Console(config-if)#map ip dscp 1 cos 0                         33-16
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                          33-20
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
⋮
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Mapping IPv6 Traffic Classes

The Traffic Class field in the IPv6 header may be used by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities for IPv6 packets. (See RFC 2460.)

Command Usage

Nodes that support a specific use of some or all of the IPv6 traffic class bits are permitted to change the value of those bits in packets that they originate, forward, or receive, as required for that specific use. Nodes should ignore and leave unchanged any bits of the traffic class field for which they do not support a specific use.

Command Attributes

- **Port** – Port identifier. (Range: 1-18)
- **IPv6 Traffic Class** – IPv6 traffic class. (Range: 0-255)
- **Priority** – Class-of-Service value (Range: 0-7)

Web – Click Priority, IPv6 Mapping. Select a port for which to set the IPv6 traffic class to CoS map, select the IPv6 traffic class and corresponding CoS value, then click Add.

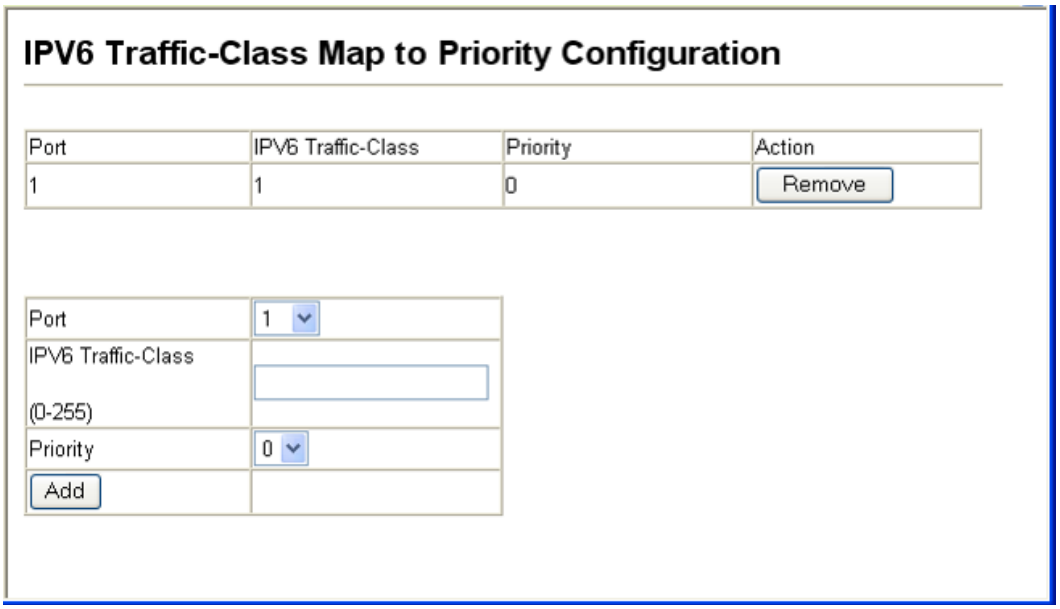


Figure 14-8 IP Port Priority Status

Downloaded from www.Manualslib.com manuals search engine

CLI – The following example maps the Traffic Class value of 1 to CoS value 0.

```
Console(config)#priority ipv6 1 0                                    33-17
Console(config)#end
Console#show priority                                                33-4
CPU TX Priority 0
PORT   Traffic-Class        Priority
1      1                    0
Console#
```

Mapping IP Port Priority

You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that "0" represents low priority and "7" represent high priority.

Note: Up to 8 entries can be specified.
IP Port Priority settings apply to all interfaces.

Web – Click Priority, IP Port Priority Status. Set IP Port Priority Status to Enabled.

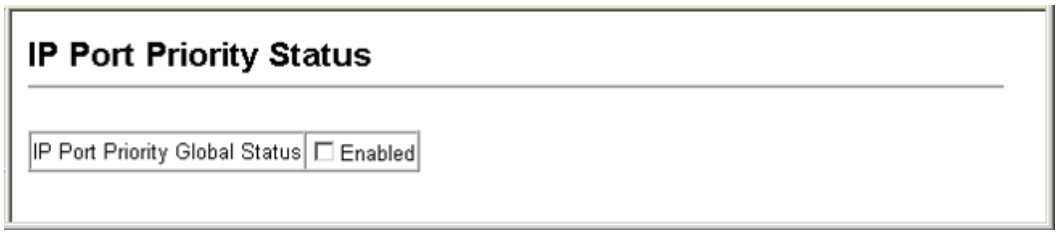


Figure 14-9 IP Port Priority Status

Downloaded from www.Manualslib.com manuals search engine

Click Priority, IP Port Priority. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Apply.

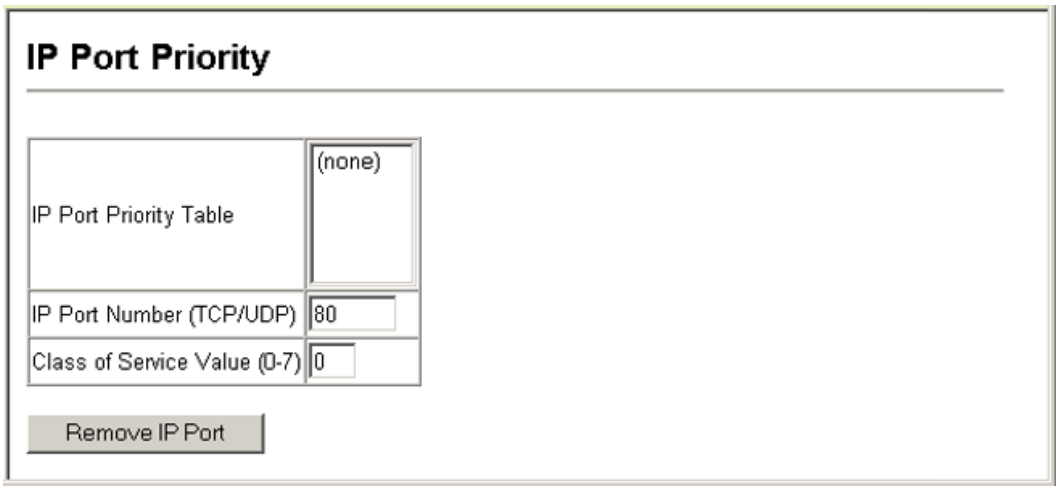


Figure 14-10 IP Port Priority

CLI – The following example globally enables IP Port Priority service on the switch, maps HTTP traffic (on port 1) to CoS value 0, and then displays the IP Port Priority settings.

```
Console(config)#map ip port                                    33-12
Console(config)#interface ethernet 1/1                         25-2
Console(config-if)#map ip port 80 cos 0                        33-12
Console(config-if)#end
Console#show map ip port ethernet 1/5                          33-17
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 1       80   0
Console#
```

* Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 15
QUALITY OF SERVICE

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Downloaded from www.Manualslib.com manuals search engine

Notes: **1.** You can configure up to 16 rules per Class Map. You can also include multiple classes in a Policy Map.

2. You should create a Class Map before creating a Policy Map. Otherwise, you will not be able to select a Class Map from the Policy Rule Settings screen (see page 15-9).

Configuring Quality of Service Parameters

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the "Class Map" to designate a class name for a specific category of traffic.
2. Edit the rules for each class to specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Set an ACL mask to enable filtering for the criteria specified in the Class Map. (See "Configuring an IP ACL Mask" on page 8-11 or "Configuring a MAC ACL Mask" on page 8-14.)
4. Use the "Policy Map" to designate a policy name for a specific manner in which ingress traffic will be handled.
5. Add one or more classes to the Policy Map. Assign policy rules to each class by "setting" the QoS value to be assigned to the matching traffic class. The policy rule can also be configured to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
6. Use the "Service Policy" to assign a policy map to a specific interface.

Downloaded from www.Manualslib.com manuals search engine

Configuring a Class Map

A class map is used for matching packets to a specified class.

Command Usage

- To configure a Class Map, follow these steps:
  - Open the Class Map page, and click Add Class.
  - When the Class Configuration page opens, fill in the "Class Name" field, and click Add.
  - When the Match Class Settings page opens, specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN, and click the Add button next to the field for the selected traffic criteria. You can only specify one item to match when assigning ingress traffic to a class map.
- The class map uses the Access Control List filtering engine, so you must also set an ACL mask to enable filtering for the criteria specified in the Class Map. See "Configuring an IP ACL Mask" on page 8-11 or "Configuring a MAC ACL Mask" on page 8-14 for information on configuring an appropriate ACL mask.
- The class map is used with a policy map (page 15-6) to create a service policy (page 15-10) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

Command Attributes

Class Map

- **Modify Name and Description** – Configures the name and a brief description of a class map. (Range: 1-16 characters for the name; 1-80 characters for the description)
- **Edit Rules** – Opens the "Match Class Settings" page for the selected class entry. Modify the criteria used to classify ingress traffic on this page.
- **Add Class** – Opens the "Class Configuration" page. Enter a class name and description on this page, and click Add to open the "Match Class

Downloaded from www.Manualslib.com manuals search engine

Settings" page. Enter the criteria used to classify ingress traffic on this web page.

- **Remove Class** – Removes the selected class.

Class Configuration

- **Class Name** – Name of the class map. (Range: 1-16 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **Description** – A brief description of a class map. (Range: 1-80 characters)
- **Add** – Adds the specified class.
- **Back** – Returns to previous page with making any changes.

Match Class Settings

- **Class Name** – List of class maps.
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN** – A VLAN. (Range:1-4093)
- **Add** – Adds specified criteria to the class. Up to 16 items are permitted per class.
- **Remove** – Deletes the selected criteria from the class.

Downloaded from www.Manualslib.com manuals search engine

Web – Click QoS, DiffServ, then click Add Class to create a new class, or Edit Rules to change the rules of an existing class.

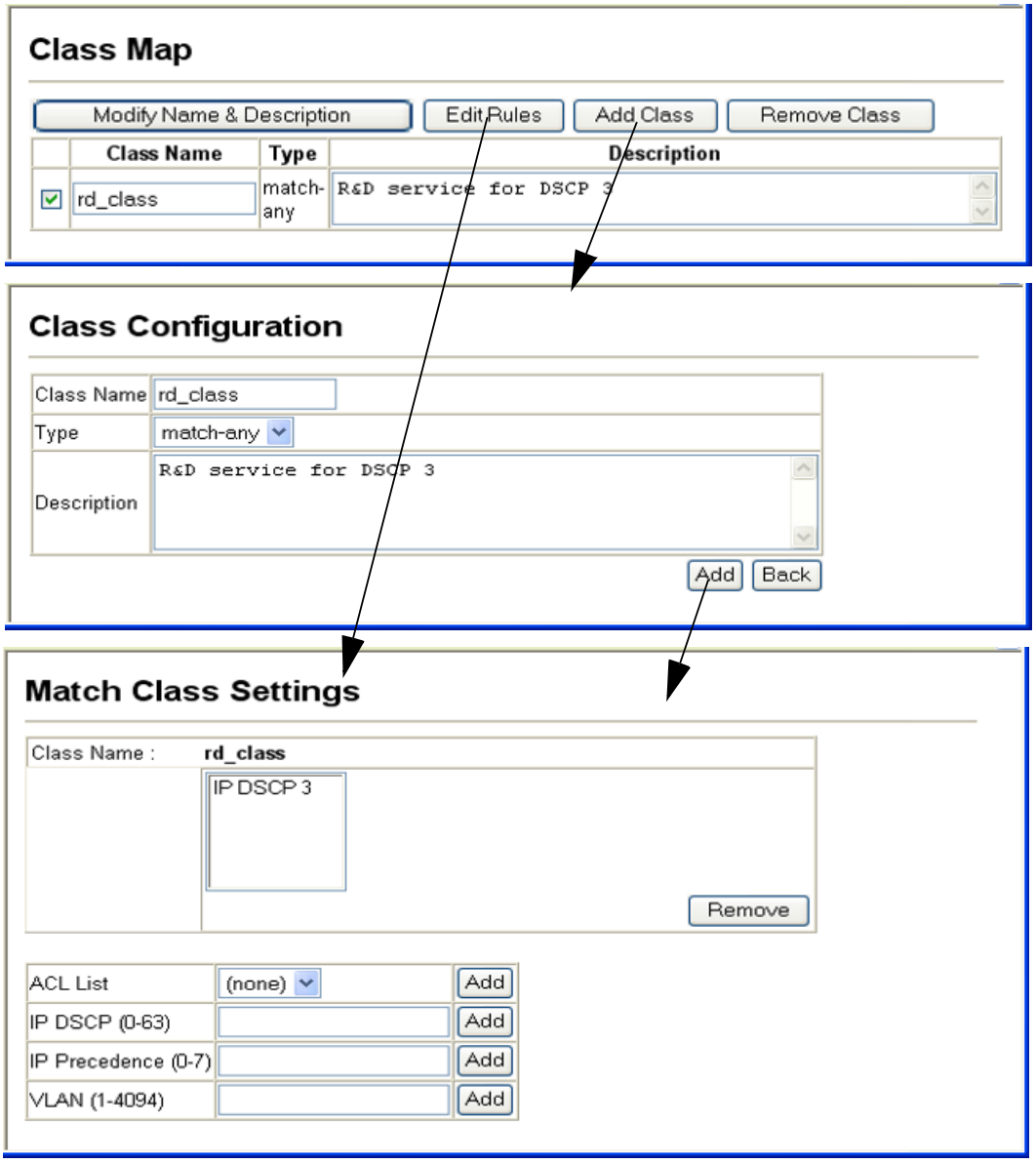


Figure 15-1 Configuring Class Maps

CLI - This example creates a class map call "rd-class," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd_class match-any                    34-3
Console(config-cmap)#match ip dscp 3                            34-4
Console(config-cmap)#
```


Downloaded from www.Manualslib.com manuals search engine

Creating QoS Policies

This function creates a policy map that can be attached to multiple interfaces.

Command Usage

- To configure a Policy Map, follow these steps:
  - Create a Class Map as described on page 15-3.
  - Open the Policy Map page, and click Add Policy.
  - When the Policy Configuration page opens, fill in the "Policy Name" field, and click Add.
  - When the Policy Rule Settings page opens, select a class name from the scroll-down list (Class Name field). Configure a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed field). Then finally click Add to register the new policy.
- A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings (page 15-10). You can configure up to 63 policers (i.e., class maps) for Fast Ethernet and Gigabit Ethernet ingress ports.

  Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the "Burst" field, and the average rate tokens are removed from the bucket is by specified by the "Rate" option.
- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 15-10) to take effect.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

Policy Map

- **Modify Name and Description** – Configures the name and a brief description of a policy map. (Range: 1-16 characters for the name; 1-80 characters for the description)
- **Edit Classes** – Opens the "Policy Rule Settings" page for the selected class entry. Modify the criteria used to service ingress traffic on this page.
- **Add Policy** – Opens the "Policy Configuration" page. Enter a policy name and description on this page, and click Add to open the "Policy Rule Settings" page. Enter the criteria used to service ingress traffic on this page.
- **Remove Policy** – Deletes a specified policy.

Policy Configuration

- **Policy Name** — Name of policy map. (Range: 1-16 characters)
- **Description** – A brief description of a policy map. (Range: 1-80 characters)
- **Add** – Adds the specified policy.
- **Back** – Returns to previous page with making any changes.

Policy Rule Settings

- Class Settings -

- **Class Name** – Name of class map.
- **Action** – Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 15-3).
- **Meter** – The maximum throughput and burst rate.
  - **Rate (kbps)** – Rate in kilobits per second.
  - **Burst (byte)** – Burst in bytes.
- **Exceed Action** – Specifies whether the traffic that exceeds the specified rate will be dropped or the DSCP service level will be reduced.

Downloaded from www.Manualslib.com manuals search engine

- **Remove Class** – Deletes a class.

- Policy Options -

- **Class Name** – Name of class map.
- **Action** – Configures the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 15-3). (Range - CoS: 0-7, DSCP: 0-63, IP Precedence: 0-7)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
  - **Rate (kbps)** – Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
  - **Burst (byte)** – Burst in bytes. (Range: 64-1522)
- **Exceed** – Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.
  - **Set** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
  - **Drop** – Drops out of conformance traffic.
- **Add** – Adds the specified criteria to the policy map.

Downloaded from www.Manualslib.com manuals search engine

Web – Click QoS, DiffServ, Policy Map to display the list of existing policy maps. To add a new policy map click Add Policy. To configure the policy rule settings click Edit Classes.

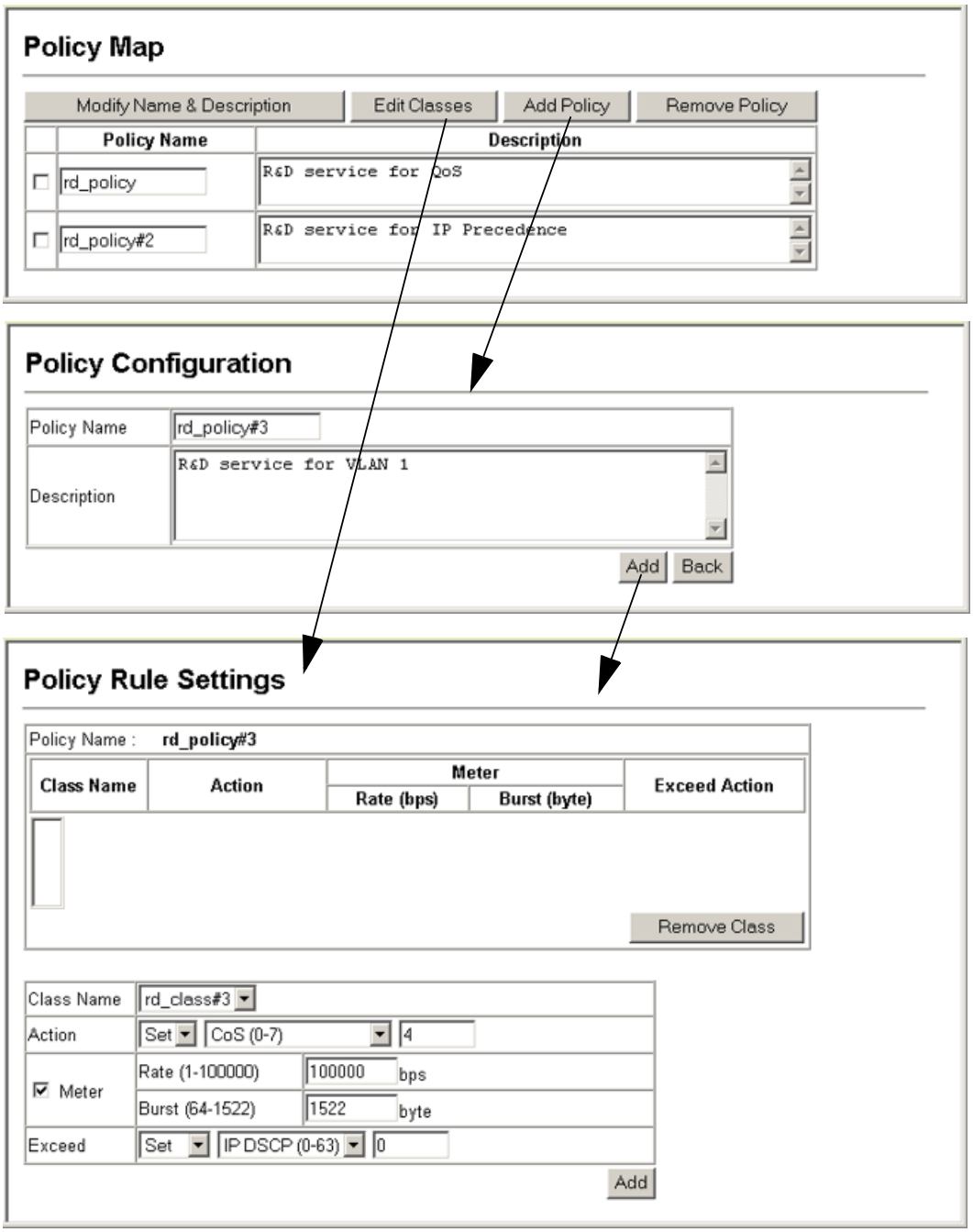


Figure 15-2 Configuring Policy Maps

Downloaded from www.Manualslib.com manuals search engine

CLI – This example creates a policy map called "rd-policy," sets the average bandwidth the 1 Mbps, the burst rate to 1522 bps, and the response to reduce the DSCP value for violating packets to 0.

```
Console(config)#policy-map rd_policy#3                          34-6
Console(config-pmap)#class rd_class#3                           34-7
Console(config-pmap-c)#set ip dscp 4                            34-8
Console(config-pmap-c)#police 100000 1522 exceed-action
  set ip dscp 0                                                 34-9
Console(config-pmap-c)#
```

Attaching a Policy Map to Ingress Queues

This function binds a policy map to the ingress queue of a particular interface.

Command Usage

- You must first define a class map, set an ACL mask to match the criteria defined in the class map, then define a policy map, and finally bind the service policy to the required interface.
- You can only bind one policy map to an interface.
- The current firmware does not allow you to bind a policy map to an egress queue.

Command Attributes

- **Ports** – Specifies a port.
- **Ingress** – Applies the rule to ingress traffic.
- **Enabled** – Check this to enable a policy map on the specified port.
- Policy Map – Select the appropriate policy map from the scroll-down box.

Downloaded from www.Manualslib.com manuals search engine

Web – Click QoS, DiffServ, Service Policy Settings. Check Enabled and choose a Policy Map for a port from the scroll-down box, then click Apply.

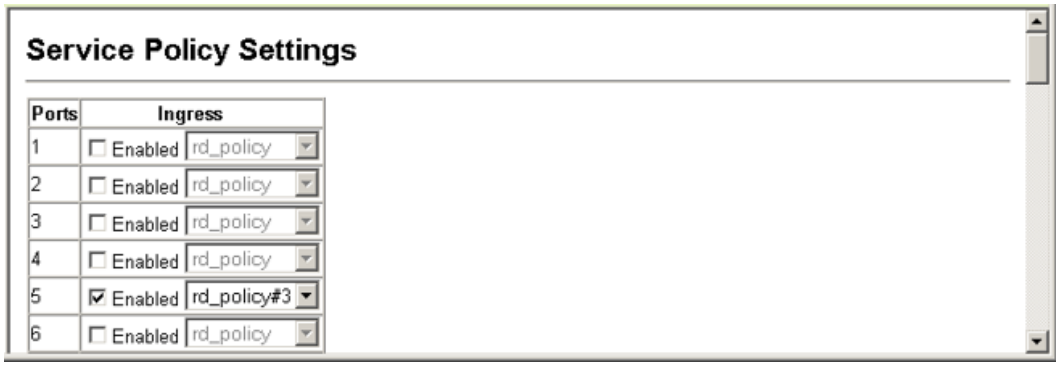


Figure 15-3 Service Policy Settings

CLI - This example applies a service policy to an ingress interface.

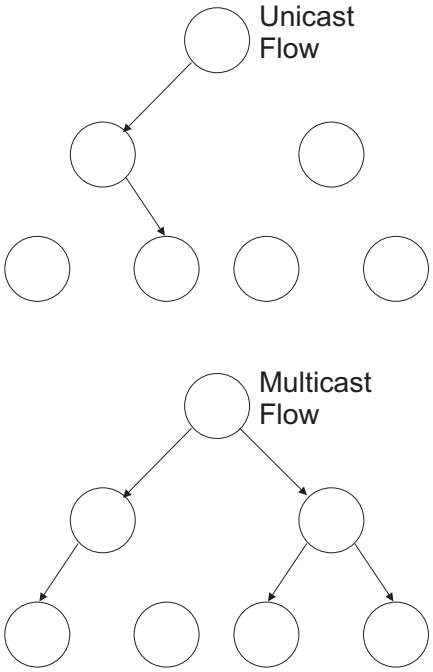
```
Console(config)#interface ethernet 1/5                    25-2
Console(config-if)#service-policy input rd_policy#3       34-10
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 16
MULTICAST FILTERING

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.



This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to

Downloaded from www.Manualslib.com manuals search engine

those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN). IGMP profile filtering can also be used to control access to specific multicast services.

You can also configure a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation "Multicast VLAN Registration" on page 16-20.

Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 16-4) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have not requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source.

Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic

Downloaded from www.Manualslib.com manuals search engine

is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from all sources except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.

Notes: **1.** When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.

2. IGMP snooping will not function unless a multicast router port is enabled on the switch. This can accomplished in one of two ways. A static router port can be manually configured (see "Specifying Static Interfaces for a Multicast Router" on page 16-8). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

3. A maximum of up to 255 multicast entries can be maintained for IGMP snooping and 255 entries for Multicast Routing when both of these features are enabled. If the table's capacity is exceeded, then IGMPv3 snooping will not support multicast source filtering, but will forward multicast traffic from all relevant sources to the requesting hosts.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 16-8). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 16-11).

Downloaded from www.Manualslib.com manuals search engine

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

Note: Unknown multicast traffic is flooded to all ports in the VLAN for several seconds when first received. If a multicast router port exists on the VLAN, the traffic will be filtered by subjecting it to IGMP snooping. If no router port exists on the VLAN or the multicast filtering table is already full, the switch will continue flooding the traffic into the VLAN.

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Downloaded from www.Manualslib.com manuals search engine

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)
- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-25 seconds, Default: 10)
- **IGMP Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Range: 1-3; Default: 2)

Notes: **1.** All systems on the subnet must support the same version.
2. Some attributes are only enabled for IGMPv2 and v3, including IGMP Report Delay and IGMP Query Timeout.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)

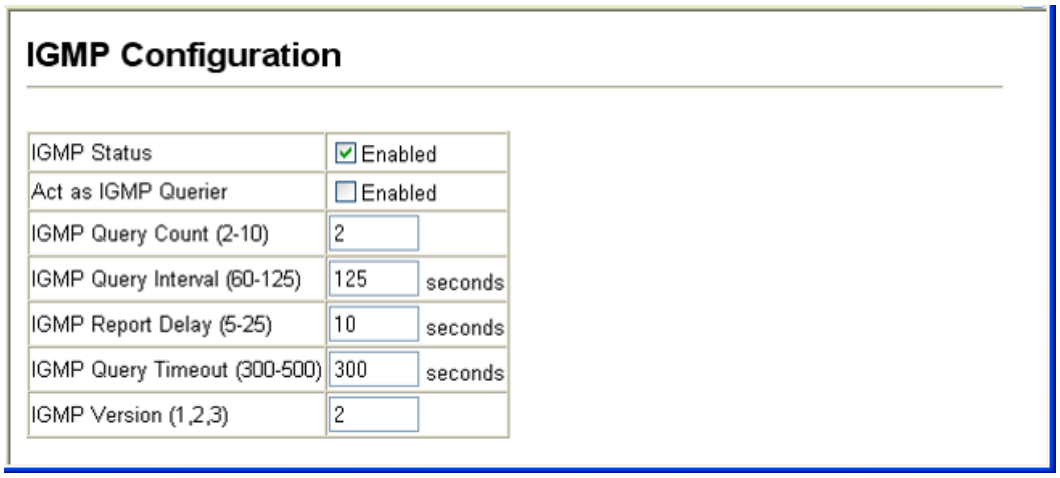


Figure 16-1 IGMP Configuration

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                                  35-2
Console(config)#ip igmp snooping querier                          35-8
Console(config)#ip igmp snooping query-count 10                   35-8
Console(config)#ip igmp snooping query-interval 100               35-9
Console(config)#ip igmp snooping query-max-response-time 20   35-10
Console(config)#ip igmp snooping router-port-expire-time 300  35-11
Console(config)#ip igmp snooping version 2                        35-4
Console(config)#exit
Console#show ip igmp snooping                                     35-6
 Service status:          Enabled
 Querier status:          Enabled
 Query count:             10
 Query interval:          100 sec
 Query max response time: 20 sec
 Router port expire time: 300 sec
 IGMP snooping version:   Version 2
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying Interfaces Attached to a Multicast Router

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.

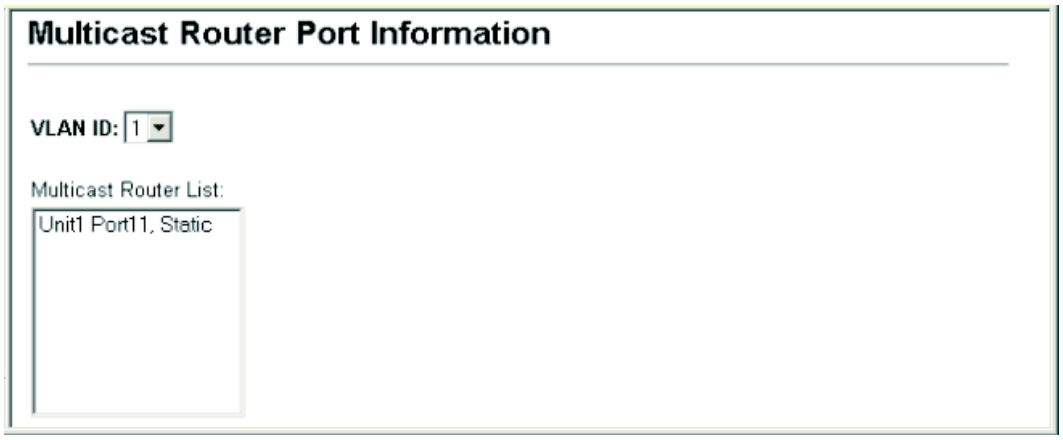


Figure 16-2 Multicast Router Port Information

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                    35-13
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
Console#
```

Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.

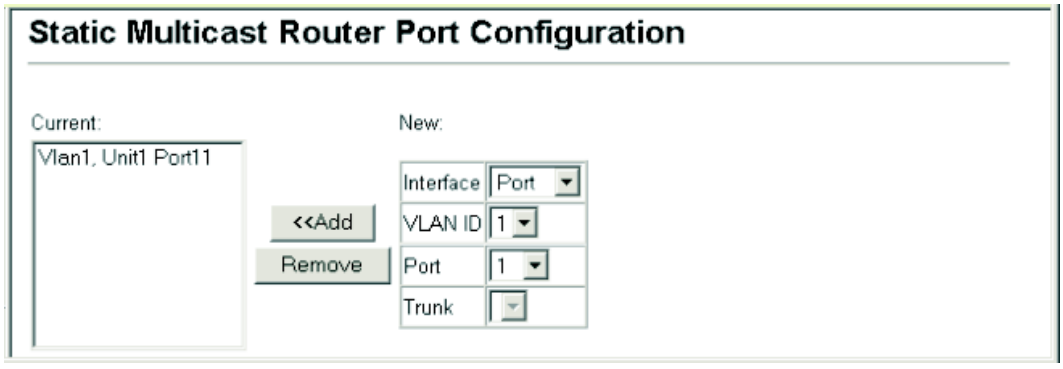


Figure 16-3 Static Multicast Router Port Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11 35-12
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                  35-13
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11  Static
Console#
```

Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attributes

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.

Figure 16-4 IP Multicast Registration Table

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

```
Console#show mac-address-table multicast vlan 1                35-6
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in "Configuring IGMP Snooping and Query Parameters" on page 16-4. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port** or **Trunk** – Specifies the interface attached to a multicast router/switch.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.

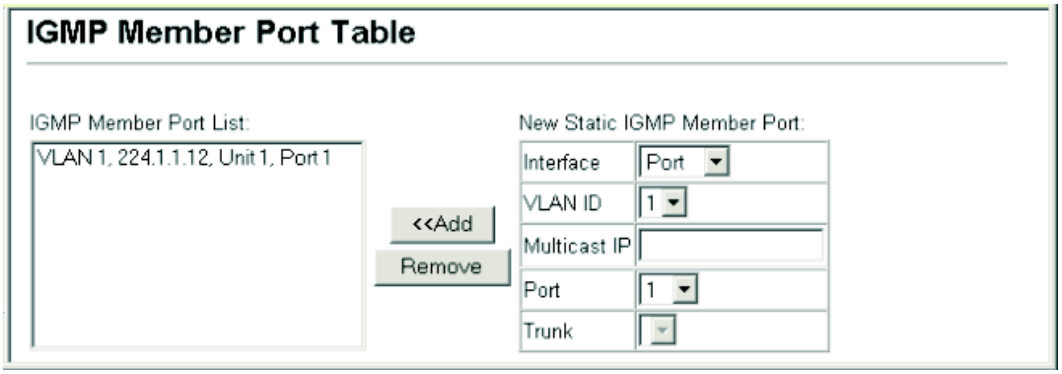


Figure 16-5 IGMP Member Port Table

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
  ethernet 1/12                                                    35-3
Console(config)#exit
Console#show mac-address-table multicast vlan 1                    35-6
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Immediate Leave from Multicast Groups

The switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the immediate-leave function is enabled for the parent VLAN.

Command Usage

- If immediate leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. Note that the timeout period is determined by the IGMP Query Report Delay (see "Configuring IGMP Snooping and Query Parameters" on page 16-4).
- If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- Immediate leave is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Command Attribute

- **VLAN ID** – VLAN Identifier. (Range: 1-4094)
- **IGMP Immediate Leave Status** – Sets the status for immediate leave on the specified VLAN. (Default: Disabled)

Downloaded from www.Manualslib.com manuals search engine

Web – Click IGMP Snooping, IGMP Immediate Leave Table. Select the VLAN interface to configure, set the status for immediate leave, and click Apply.

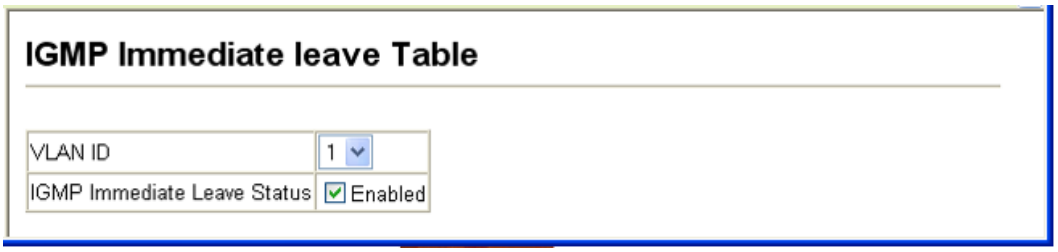


Figure 16-6 IGMP Immediate Leave Table

CLI – This example enables immediate leave on VLAN 1.

```
Console(config)#interface vlan 1                                    25-2
Console(config-if)#ip igmp snooping immediate-leave                 35-5
Console(config-if)#
```

IGMP Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multcast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

Downloaded from www.Manualslib.com manuals search engine

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Note: IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

Enabling IGMP Filtering and Throttling

To implement IGMP filtering and throttling on the switch, you must first enable the feature globally and create IGMP profile numbers.

Command Attributes

- **IGMP Filter** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)
- **IGMP Profile** – Creates IGMP profile numbers. (Range: 1-4294967295)

Web – Click IGMP Snooping, IGMP Filter Configuration. Create a profile group by entering the number in text box and clicking Add. Enable the IGMP filter status, then click Apply.

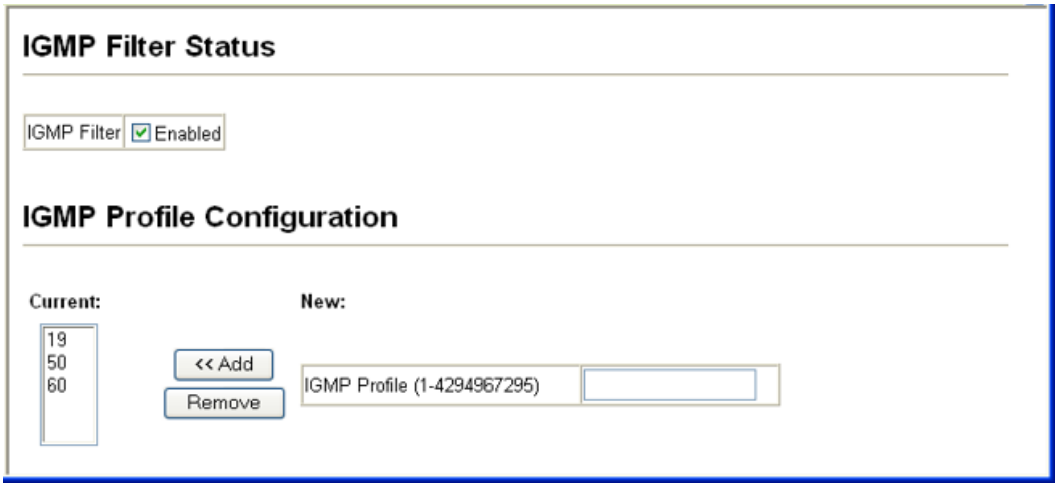


Figure 16-7 Enabling IGMP Filtering and Throttling

Downloaded from www.Manualslib.com manuals search engine

CLI – This example enables IGMP filtering and creates a profile number. It then displays the current status and the existing profile numbers.

```
Console(config)#ip igmp filter                                    35-15
Console(config)#ip igmp profile 19                                35-16
Console(config-igmp-profile)#end
Console#show ip igmp filter                                       35-20
IGMP filter enable
Console#show ip igmp profile                                      35-21
IGMP Profile 19
IGMP Profile 50
Console#
```

Configuring IGMP Filter Profiles

When you have created an IGMP profile number, you can then configure the multicast groups to filter and set the access mode.

Command Usage

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Command Attributes

- **Profile ID** – Selects an existing profile number to configure. After selecting an ID number, click the Query button to display the current configuration.
- **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)
- **New Multicast Address Range List** – Specifies multicast groups to include in the profile. Specify a multicast group range by entering a start and end IP address. Specify a single multicast group by entering the same IP address for the start and end of the range. Click the Add button to add a range to the current list.

Downloaded from www.Manualslib.com manuals search engine

- **Current Multicast Address Range List** – Lists multicast groups currently included in the profile. Select an entry and click the Remove button to delete it from the list.

Web – Click IGMP Snooping, IGMP Profile Group Configuration. Select the profile number you want to configure; then click Query to display the current settings. Specify the access mode for the profile and then add multicast groups to the profile list. Click Apply.

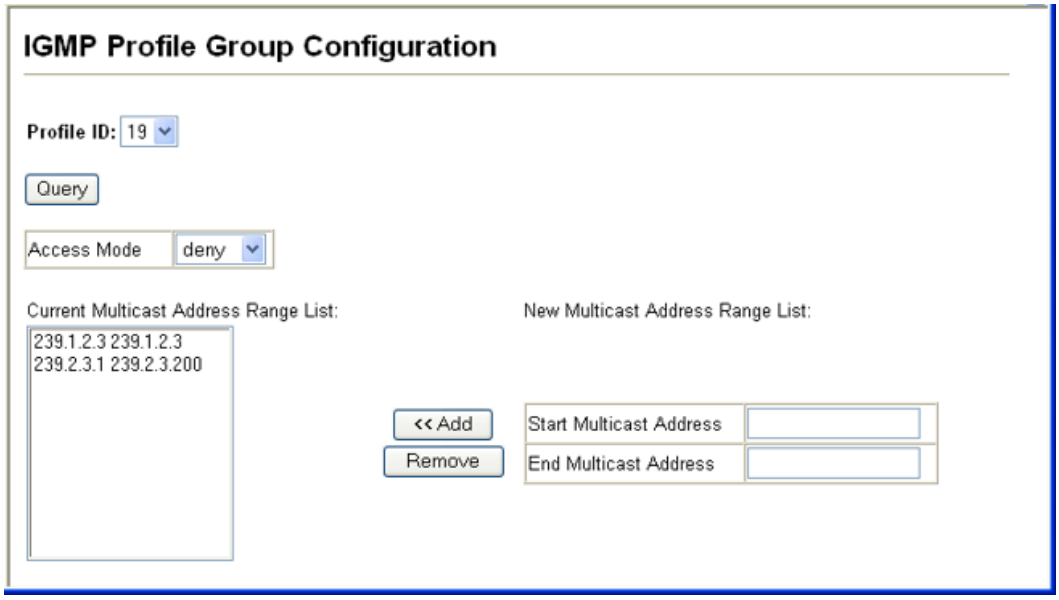


Figure 16-8 IGMP Profile Configuration

CLI – This example configures profile number 19 by setting the access mode to "permit" and then specifying a range of multicast groups that a user can join. The current profile configuration is then displayed.

```
Console(config)#ip igmp profile 19                              35-16
Console(config-igmp-profile)#permit                             35-16
Console(config-igmp-profile)#range 239.1.2.3                    35-17
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.200
Console(config-igmp-profile)#end
Console#show ip igmp profile 19                                 35-21
IGMP Profile 19
  permit
  range 239.1.2.3 239.1.2.3
  range 239.2.3.1 239.2.3.200
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IGMP Filtering and Throttling for Interfaces

Once you have configured IGMP profiles, you can assign them to interfaces on the switch. Also, you can set the IGMP throttling number to limit the number of multicast groups an interface can join at the same time.

Command Usage

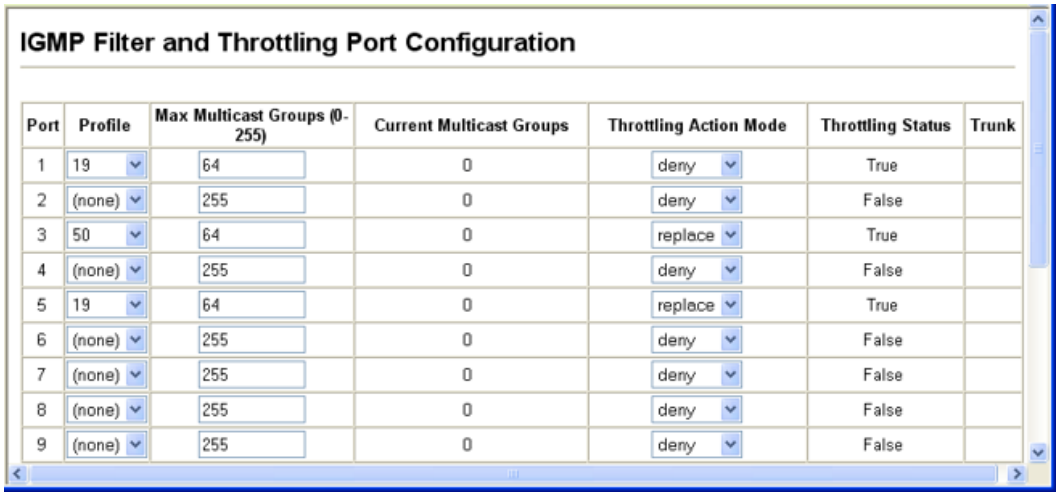
- Only one profile can be assigned to an interface.
- An IGMP profile or throttling setting can also be applied to a trunk interface. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.
- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Command Attributes

- **Profile** – Selects an existing profile number to assign to an interface.
- **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 0-255; Default: 255)
- **Current Multicast Groups** – Displays the current number of multicast groups the interface has joined.
- **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)
  - **deny** - The new multicast group join report is dropped.
  - **replace** - The new multicast group replaces an existing group.
- **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)
- **Trunk** – Indicates if a port is a trunk member.

Downloaded from www.Manualslib.com manuals search engine

Web – Click IGMP Snooping, IGMP Filter/Throttling Port Configuration or IGMP Filter/Throttling Trunk Configuration. Select a profile to assign to an interface, then set the throttling number and action. Click Apply.



IGMP Filter and Throttling Port Configuration

Port	Profile	Max Multicast Groups (0-255)	Current Multicast Groups	Throttling Action Mode	Throttling Status	Trunk
1	19	64	0	deny	True	
2	(none)	255	0	deny	False	
3	50	64	0	replace	True	
4	(none)	255	0	deny	False	
5	19	64	0	replace	True	
6	(none)	255	0	deny	False	
7	(none)	255	0	deny	False	
8	(none)	255	0	deny	False	
9	(none)	255	0	deny	False	

Figure 16-9 IGMP Filter and Throttling Port Configuration

CLI – This example assigns IGMP profile number 19 to port 1, and then sets the throttling number and action. The current IGMP filtering and throttling settings for the interface are then displayed.

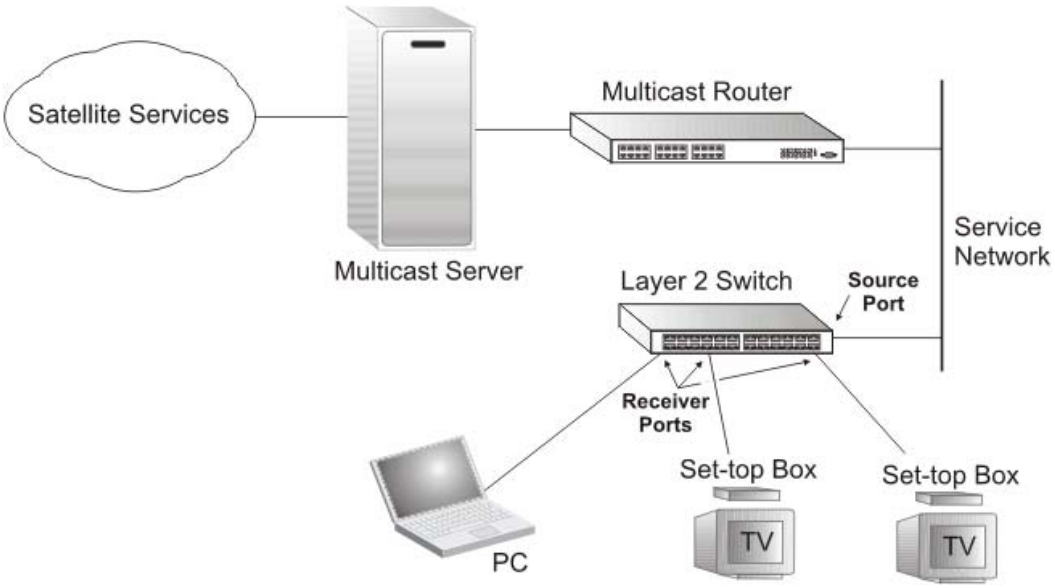
```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19                          35-16
Console(config-if)#ip igmp max-groups 64                      35-18
Console(config-if)#ip igmp max-groups action deny             35-19
Console(config-if)#end
Console#show ip igmp filter interface ethernet 1/1            35-20
Information of Eth 1/1
 IGMP Profile 19
  deny
  range 239.1.2.3 239.1.2.3
  range 239.2.3.1 239.2.3.200
Console#show ip igmp throttle interface ethernet 1/1          35-22
Information of Eth 1/1
  status : FALSE
  action : deny
  max multicast groups : 64
  current multicast groups : 1
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Multicast VLAN Registration

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast routing protocol.

MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).



Downloaded from www.Manualslib.com manuals search engine

General Configuration Guidelines for MVR

1. Enable MVR globally on the switch, select the MVR VLAN, and add the multicast groups that will stream traffic to attached hosts (see "Configuring Global MVR Settings" on page 16-21).
2. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR Interfaces" on page 16-26).
3. Enable IGMP Snooping to a allow a subscriber to dynamically join or leave an MVR group (see "Configuring IGMP Snooping and Query Parameters" on page 4). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.
4. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see "Assigning Static Multicast Groups to Interfaces" on page 16-30).

Configuring Global MVR Settings

The global settings for Multicast VLAN Registration (MVR) include enabling or disabling MVR for the switch, selecting the VLAN that will serve as the sole channel for common multicast streams supported by the service provider, and assigning the multicast group address for each of these services to the MVR VLAN.

Command Usage

- The following restrictions apply to the use of MVR domains:
  - MVR groups cannot overlap MVR domains.
  - The same VLAN cannot be assigned to different MVR domains.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see "Configuring IGMP Snooping and Query Parameters" on page 16-4). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.
- IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

Downloaded from www.Manualslib.com manuals search engine

Field Attributes

- **MVR Domain** – An independent multicast domain. (Range: 1-3; Default: 1)
- **MVR Status** – When MVR is enabled on both the switch, any multicast data associated an MVR group is sent from all designated source ports, and to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.)
- **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. (Range: 1-4094; Default: 1)
- **MVR Max Multicast Groups** – Shows the maximum number of multicast groups which can assigned to the MVR VLAN.
- **MVR Current Multicast Groups** – Shows the number of multicast groups currently assigned to the MVR VLAN.
- **MVR Group IP** – IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255; Default: no groups are assigned to the MVR VLAN)

  The IP address range of 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- **Count** – The number of contiguous MVR group addresses. (Range: 1-255; Default: 0)

Downloaded from www.Manualslib.com manuals search engine

Web – Click MVR, Configuration. Select the MVR domain, enable MVR globally on the switch, select the MVR VLAN, add the multicast groups that will stream traffic to attached hosts, and then click Apply.

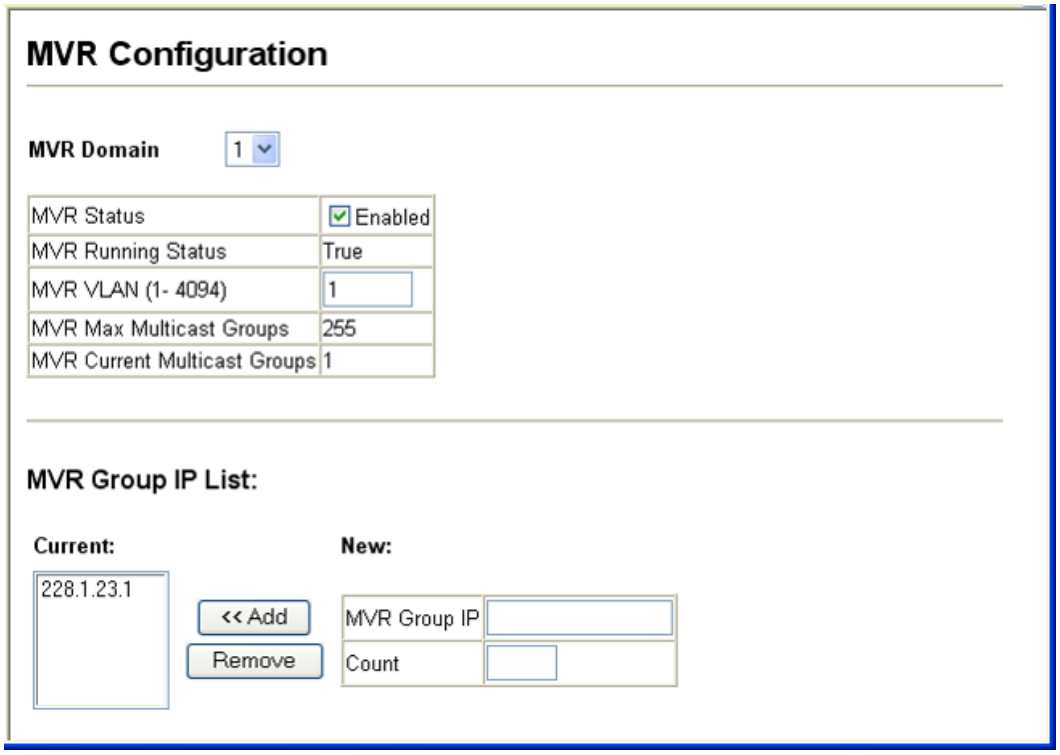


Figure 16-10 MVR Global Configuration

CLI – This example first enables IGMP snooping, enables MVR globally, and then configures a range of MVR group addresses.

```
Console(config)#ip igmp snooping                                    35-2
Console(config)#mvr                                                 35-24
Console(config)#mvr group 228.1.23.1
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

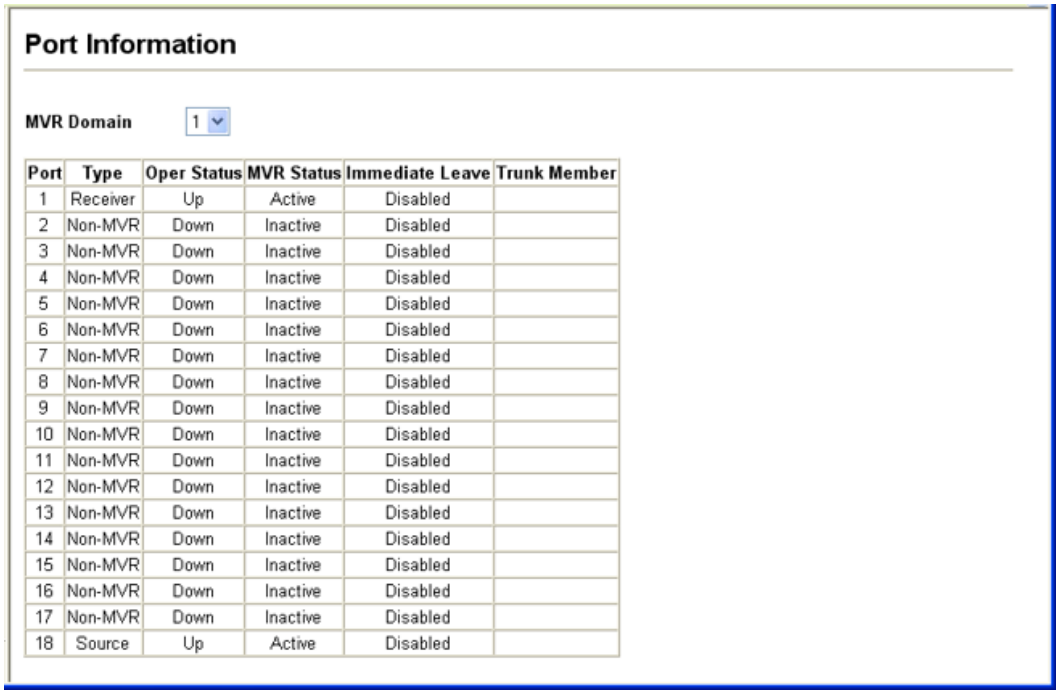
Displaying MVR Interface Status

You can display information about the interfaces attached to the MVR VLAN.

Field Attributes

- **MVR Domain** – An independent multicast domain.
- **Type** – Shows the MVR port type.
- **Oper Status** – Shows the link status.
- **MVR Status** – Shows the MVR status. MVR status for source ports is "ACTIVE" if MVR is globally enabled on the switch. MVR status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
- **Immediate Leave** – Shows if immediate leave is enabled or disabled.
- **Trunk Member**[24] – Shows if port is a trunk member.

Web – Click MVR, Port Information or Trunk Information.



Port	Type	Oper Status	MVR Status	Immediate Leave	Trunk Member
1	Receiver	Up	Active	Disabled	
2	Non-MVR	Down	Inactive	Disabled	
3	Non-MVR	Down	Inactive	Disabled	
4	Non-MVR	Down	Inactive	Disabled	
5	Non-MVR	Down	Inactive	Disabled	
6	Non-MVR	Down	Inactive	Disabled	
7	Non-MVR	Down	Inactive	Disabled	
8	Non-MVR	Down	Inactive	Disabled	
9	Non-MVR	Down	Inactive	Disabled	
10	Non-MVR	Down	Inactive	Disabled	
11	Non-MVR	Down	Inactive	Disabled	
12	Non-MVR	Down	Inactive	Disabled	
13	Non-MVR	Down	Inactive	Disabled	
14	Non-MVR	Down	Inactive	Disabled	
15	Non-MVR	Down	Inactive	Disabled	
16	Non-MVR	Down	Inactive	Disabled	
17	Non-MVR	Down	Inactive	Disabled	
18	Source	Up	Active	Disabled	

Figure 16-11 MVR Port Information

24. Port Information only.

Downloaded from www.Manualslib.com manuals search engine

CLI – This example shows information about interfaces attached to the MVR VLAN.

```
Console#show mvr interface                                        35-29
=====================================================
MVR domain : 1
Port    Type            Status          Immediate Leave
------- --------        -------------   ---------------
eth1/1  RECEIVER        ACTIVE/UP         Disable
eth1/18 SOURCE          ACTIVE/UP         Disable
:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring MVR Interfaces

Each interface that participates in the MVR VLAN must be configured as an MVR source port or receiver port. If only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

Command Usage

- MVR source ports and receiver ports can be members of more than on MVR domain. However, an interface cannot be receiver port in one MVR domain and a source port in another domain.
- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- Receiver ports can belong to different VLANs. IGMP snooping can be used to allow a receiver port to dynamically join or leave multicast groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port (see "Assigning Static Multicast Groups to Interfaces" on page 16-30). However, if a receiver port is statically configured as a member of an MVR VLAN, its status will be inactive. Also, note that VLAN membership for MVR receiver ports cannot be set to trunk mode (see "Configuring VLAN Behavior for Interfaces" on page 13-15).
- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through IGMP snooping or which have been statically assigned (see "Assigning Static Multicast Groups to Interfaces" on page 16-30).
- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

Downloaded from www.Manualslib.com manuals search engine

- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- Immediate leave does not apply to multicast groups which have been statically assigned to a port.
- Immediate leave applies to all MVR domains.

Command Attributes

- **MVR Domain** – An independent multicast domain. (Range: 1-3; Default: 1)
- **MVR Type** – The following interface types are supported:
  - Source – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN.
  - Receiver – A subscriber port that can receive multicast data sent through the MVR VLAN.
  - Non-MVR – An interface that does not participate in the MVR VLAN. (This is the default type.)
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)
- **Trunk**[25] – Shows if port is a trunk member.

25. Port Information only.

Downloaded from www.Manualslib.com manuals search engine

Web – Click MVR, Port Configuration or Trunk Configuration.

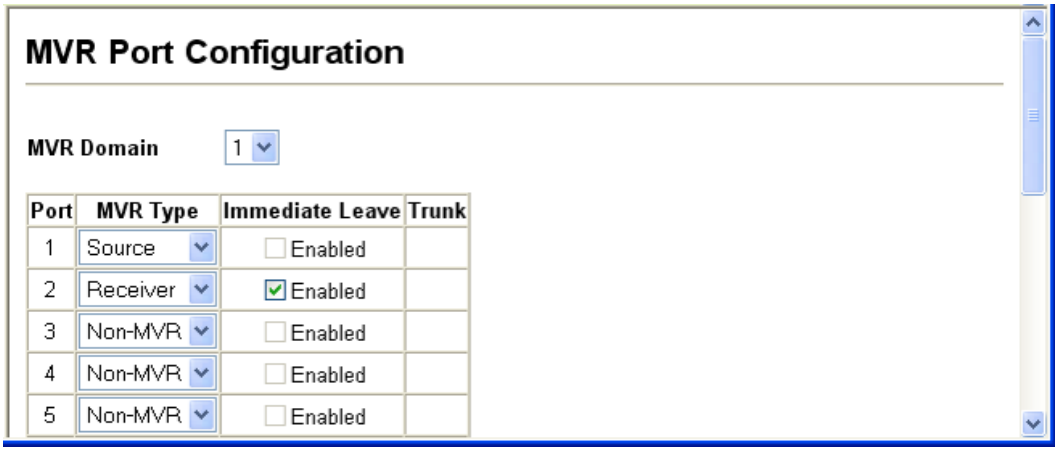


Figure 16-12 MVR Port Configuration

CLI – This example configures an MVR source port and receiver port, and then enables immediate leave on the receiver port.

```
Console(config)#interface ethernet 1/1                    25-2
Console(config-if)#mvr type source                        35-26
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#mvr type receiver
Console(config-if)#mvr immediate
Console(config-if)#
```

Displaying Port Members of Multicast Groups

You can display the multicast groups assigned to the MVR VLAN either through IGMP snooping or static configuration.

Field Attributes

- **MVR Domain** – An independent multicast domain.
- **Group IP** – Multicast groups assigned to the MVR VLAN.
- **Group Port List** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.

Downloaded from www.Manualslib.com manuals search engine

Web – Click MVR, Group IP Information.

Figure 16-13 MVR Group IP Information

CLI – This example following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN.

```
Console#show mvr members                                          35-29
MVR Group IP      Status    Members
----------------  --------  -------
225.0.0.1         ACTIVE    eth1/1(s), eth1/18(d)
225.0.0.2         INACTIVE  None
225.0.0.3         INACTIVE  None
225.0.0.4         INACTIVE  None
225.0.0.5         INACTIVE  None
225.0.0.6         INACTIVE  None
225.0.0.7         INACTIVE  None
225.0.0.8         INACTIVE  None
225.0.0.9         INACTIVE  None
225.0.0.10        INACTIVE  None
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Assigning Static Multicast Groups to Interfaces

For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces.

Command Usage

- Any multicast groups that use the MVR VLAN must be statically assigned to it under the MVR Configuration menu (see "Configuring Global MVR Settings" on page 16-21).
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

Command Attributes

- **MVR Domain** – An independent multicast domain. (Range: 1-3; Default: 1)
- **Interface** – Indicates a port or trunk.
- **Member** – Shows the IP addresses for MVR multicast groups which have been statically assigned to the selected interface.
- **Non-Member** – Shows the IP addresses for all MVR multicast groups which have not been statically assigned to the selected interface.

Downloaded from www.Manualslib.com manuals search engine

Web – Click MVR, Group Member Configuration. Select a port or trunk from the "Interface" field, and click Query to display the assigned multicast groups. Select a multicast address from the displayed lists, and click the Add or Remove button to modify the Member list.

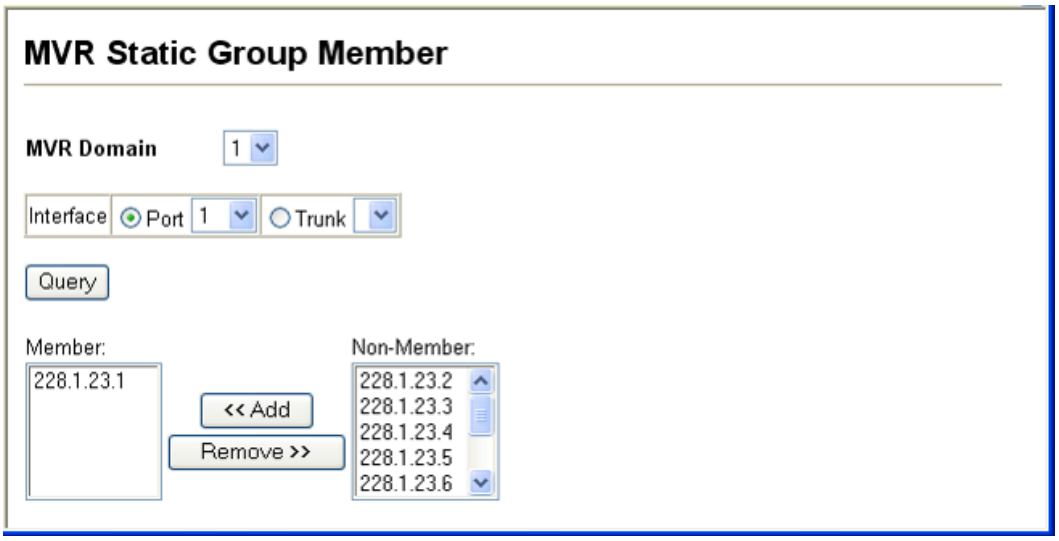


Figure 16-14 MVR Group Member Configuration

CLI – This example statically assigns a multicast group to a receiver port.

```
Console(config)#interface ethernet 1/2                    25-2
Console(config-if)#mvr group 228.1.23.1                   35-26
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 17
DOMAIN NAME SERVICE

The Domain Naming System (DNS) service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Configuring General DNS Service Parameters

Command Usage

- To enable DNS service on this switch, configure one or more name servers, and enable domain lookup status.
- To append domain names to incomplete host names received from a DNS client (i.e., not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.
- If there is no domain list, the default domain name is used. If there is a domain list, the system will search it for a corresponding entry. If none is found, it will use the default domain name.
- When an incomplete host name is received by the DNS service on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.

Downloaded from www.Manualslib.com manuals search engine

- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- If all name servers are deleted, DNS will automatically be disabled. This is done by disabling the domain lookup status.

Command Attributes

- **Domain Lookup Status** – Enables DNS host name-to-address translation.
- **Default Domain Name**[26] – Defines the default domain name appended to incomplete host names. (Range: 1-63 alphanumeric characters)
- **Domain Name List**[26] – Defines a list of domain names that can be appended to incomplete host names. (Range: 1-63 alphanumeric characters. 1-3 names)
- **Name Server List** – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

26. Do not include the initial dot that separates the host name from the domain name.

Downloaded from www.Manualslib.com manuals search engine

Web – Select DNS, General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use to use for address resolution, enable domain lookup status, and click Apply.

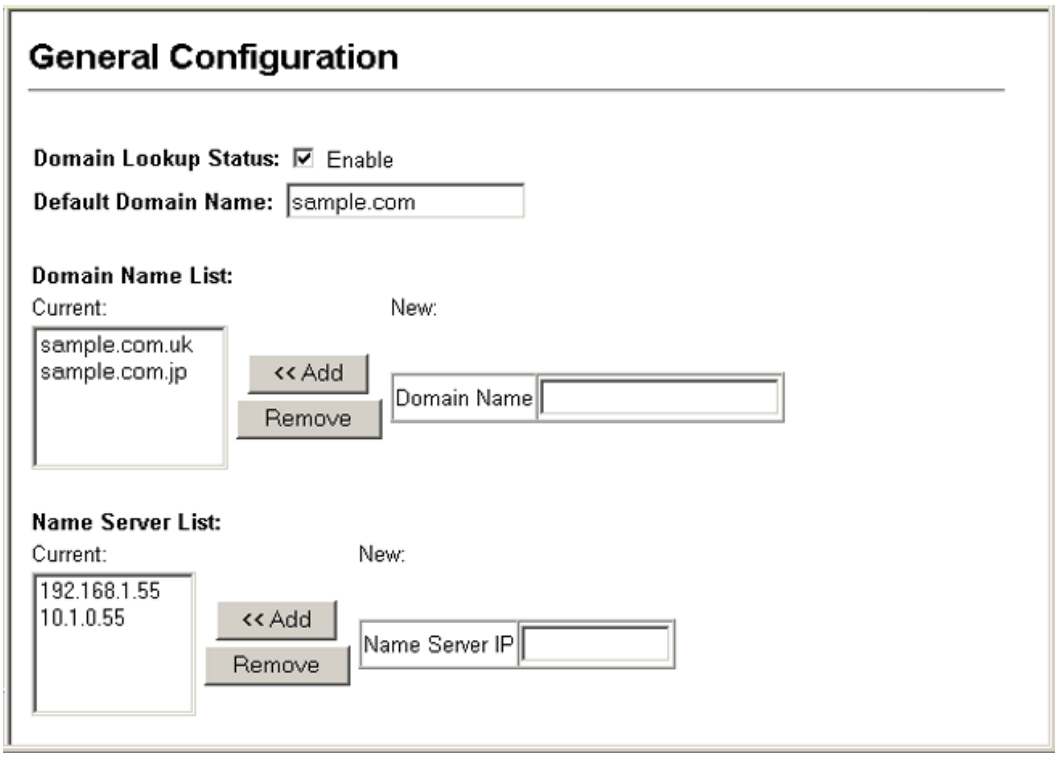


Figure 17-1 DNS General Configuration

Downloaded from www.Manualslib.com manuals search engine

CLI - This example sets a default domain name and a domain list. However, remember that if a domain list is specified, the default domain name is not used.

```
Console(config)#ip domain-name sample.com                    36-4
Console(config)#ip domain-list sample.com.uk                 36-5
Console(config)#ip domain-list sample.com.jp
Console(config)#ip name-server 192.168.1.55 10.1.0.55        36-6
Console(config)#ip domain-lookup                             36-7
Console(config)#end
Console#show dns                                             36-9
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.uk
    sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Configuring Static DNS Host to Address Entries

You can manually configure static entries in the DNS table that are used to map domain names to IP addresses.

Command Usage

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.
- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Downloaded from www.Manualslib.com manuals search engine

Field Attributes

- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)
- **IP Address** – Internet address(es) associated with a host name. (Range: 1-8 addresses)
- **Alias** – Displays the host names that are mapped to the same address(es) as a previously configured entry.

Web – Select DNS, Static Host Table. Enter a host name and one or more corresponding addresses, then click Apply.

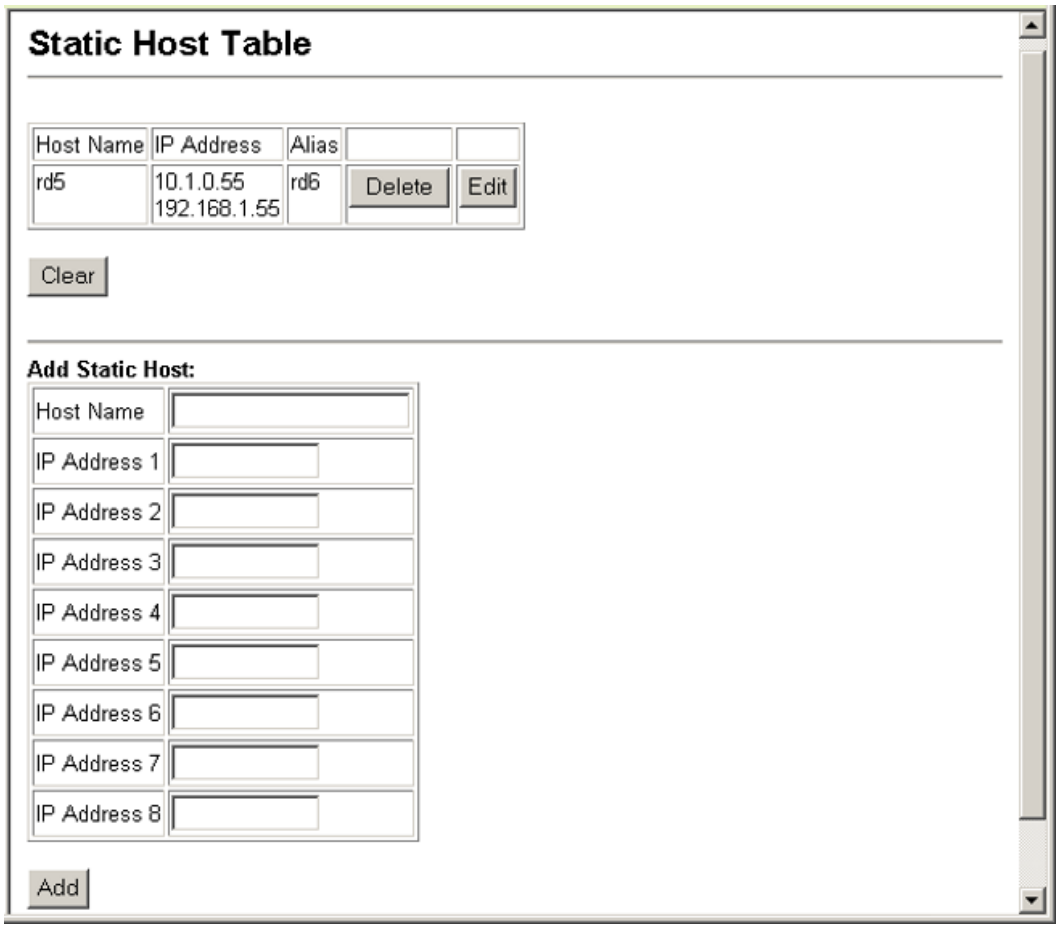


Figure 17-2 DNS Static Host Table

Downloaded from www.Manualslib.com manuals search engine

CLI - This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55            36-2
Console(config)#end
Console#show hosts                                            36-8

Hostname
 rd5
Inet address
 192.168.1.55 10.1.0.55
Console#
```

Displaying the DNS Cache

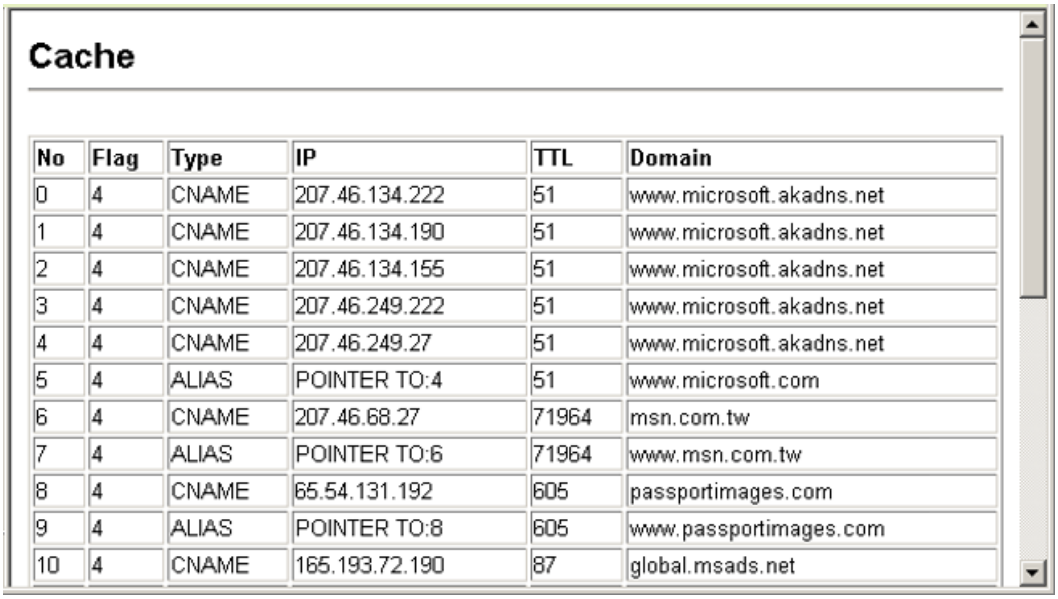
You can display entries in the DNS cache that have been learned via the designated name servers.

Field Attributes

- **No** – The entry number for each resource record.
- **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

Downloaded from www.Manualslib.com manuals search engine

Web – Select DNS, Cache.



Cache

No	Flag	Type	IP	TTL	Domain
0	4	CNAME	207.46.134.222	51	www.microsoft.akadns.net
1	4	CNAME	207.46.134.190	51	www.microsoft.akadns.net
2	4	CNAME	207.46.134.155	51	www.microsoft.akadns.net
3	4	CNAME	207.46.249.222	51	www.microsoft.akadns.net
4	4	CNAME	207.46.249.27	51	www.microsoft.akadns.net
5	4	ALIAS	POINTER TO:4	51	www.microsoft.com
6	4	CNAME	207.46.68.27	71964	msn.com.tw
7	4	ALIAS	POINTER TO:6	71964	www.msn.com.tw
8	4	CNAME	65.54.131.192	605	passportimages.com
9	4	ALIAS	POINTER TO:8	605	www.passportimages.com
10	4	CNAME	165.193.72.190	87	global.msads.net

Figure 17-3 DNS Cache

CLI - This example displays all the resource records learned from the designated name servers.

```
Console#show dns cache                                              36-9
NO       FLAG     TYPE     IP              TTL      DOMAIN
0          4      CNAME    207.46.134.222  51       www.microsoft.akadns.net
1          4      CNAME    207.46.134.190  51       www.microsoft.akadns.net
2          4      CNAME    207.46.134.155  51       www.microsoft.akadns.net
3          4      CNAME    207.46.249.222  51       www.microsoft.akadns.net
4          4      CNAME    207.46.249.27   51       www.microsoft.akadns.net
5          4      ALIAS    POINTER TO:4    51       www.microsoft.com
6          4      CNAME    207.46.68.27    71964    msn.com.tw
7          4      ALIAS    POINTER TO:6    71964    www.msn.com.tw
8          4      CNAME    65.54.131.192   605      passportimages.com
9          4      ALIAS    POINTER TO:8    605      www.passportimages.com
10         4      CNAME    165.193.72.190  87       global.msads.net
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

SECTION III
COMMAND LINE INTERFACE

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

Overview of the Command Line Interface 18-1
General Commands 19-1
System Management Commands 20-1
SNMP Commands 21-1
User Authentication Commands 22-1
Client Security Commands 23-1
Access Control List Commands 24-1
Interface Commands 25-1
Link Aggregation Commands 26-1
Mirror Port Commands 27-1
Rate Limit Commands 28-1
VDSL Commands 29-1
Address Table Commands 30-1
Spanning Tree Commands 31-1
VLAN Commands 32-1
Class of Service Commands 33-1
Quality of Service Commands 34-1
Multicast Filtering Commands 35-1
Domain Name Service Commands 36-1
DHCP Commands 37-1

Downloaded from www.Manualslib.com manuals search engine

IP Interface Commands 38-1

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 18
OVERVIEW OF THE COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "quit" or "exit" command.

Downloaded from www.Manualslib.com manuals search engine

After connecting to the system through the console port, the login screen displays:

```
User Access Verification
Username: admin
Password:

      CLI session with the SMC7816M/VSW is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.

Downloaded from www.Manualslib.com manuals search engine

2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the SMC7816M/VSW is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.

Downloaded from www.Manualslib.com manuals search engine

- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "logging history" example, typing **log** followed by a tab will result in printing the command up to "**logging**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Downloaded from www.Manualslib.com manuals search engine

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, Interface, Line, or VLAN Database, or MSTP). You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  access-group        Access groups
  access-list         Access lists
  bme                 Bme
  bridge-ext          Bridge extend information
  calendar            Date information
  class-map           Display class maps
  cpe                 Display the status of CPE connected to a port
  cpe-ethernet        Display the status of CPE connected to a port
  cpe-info          Display the system info of CPE connected to a port
  cpu                 CPU information
  dns                 DNS information
  dot1q-tunnel        Dot1q-tunnel information
  dot1x               Show 802.1x content
  filter              Confirms configuration about filtering function
  garp                GARP property
  gvrp                Show GARP information of interface
  history             Information of history
  hosts               Host information
  interfaces          Information of interfaces
  ip                  IP information
  lacp                Show LACP statistic
  line                TTY line information
  log                 Login records
  logging             Show the contents of logging buffers
  lre                 Display the status of VDSL2 line
  mac                 MAC access lists
  mac-address-table   Set configuration of the address table
  management          Show management IP filter
  map                 Map priority
  memory              Memory information
  mvr                 Display the MVR information
  policy-map          Display policy maps
  port                Characteristics of the port
  priority            Confirms configuration about priority function
  protocol-vlan       Protocol-VLAN information
  public-key          Show information of public key
  pvlan               Information of private VLAN
  queue               Information of priority queue
  radius-server       RADIUS server information
  rate-limit          Display rate limit information
  running-config      The system configuration of running
  snmp                SNMP statistics
```


Downloaded from www.Manualslib.com manuals search engine

```
  sntp                SNTP
  spanning-tree       Specify spanning-tree
  ssh                 Secure shell
  startup-config      The system configuration of starting up
  system              Information of system
  tacacs-server       Login by TACACS server
  users               Display information about terminal lines
  version             System hardware and software status
  vlan                Switch VLAN Virtual Interface
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  counters        Information of interfaces counters
  efm             Efm
  protocol-vlan   Protocol-vlan information
  status          Information of interfaces status
  switchport      Information of interfaces switchport
Console#
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp            sntp            spanning-tree   ssh
startup-config  system
Console#sh s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Downloaded from www.Manualslib.com manuals search engine

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 18-1 General Command Modes

Class	Mode	
Exec	Normal, Privileged	
Configuration	Global*	Access Control List Class Map IGMP Profile Interface Line Multiple Spanning Tree Policy Map VLAN Database VDSL Line Profile VDSL Alarm Profile

* You must be in Privileged Exec mode to access the Global configuration mode. You must be in Global Configuration mode to access any of the other configuration modes.

Downloaded from www.Manualslib.com manuals search engine

Exec Commands

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password "admin." The system will now display the "Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password "super" (page 22-4).

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

      CLI session with the SMC7816M/VSW is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
 Username: guest
 Password: [guest login password]

       CLI session with the SMC7816M/VSW is opened.
       To end the CLI session, enter [Exit].

 Console>enable
 Password: [privileged level password]
 Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

Downloaded from www.Manualslib.com manuals search engine

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- VLAN Configuration - Includes the command to create VLAN groups.
- VDSL Line Profile - Creates a profile of configuration settings that can be applied to a group of VDSL ports.
- VDSL Alarm Profile - Creates a profile of alarm thresholds that can be applied globally to the switch or to a group of VDSL ports.
- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 18-2 Configuration Command Modes

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)#	20-27
Access Control List	access-list ip standard access-list ip extended access-list ip mask-precedence access-list mac access-list mac mask-precedence	Console(config-std-acl) Console(config-ext-acl) Console(config-ip-mask-acl) Console(config-mac-acl) Console(config-mac-mask-acl)	24-3 24-3 24-8 24-17 24-20
Class Map	class map	Console(config-cmap)	34-3
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)	25-2
MSTP	spanning-tree mst-configuration	Console(config-mstp)	31-10
Policy Map	policy map	Console(config-pmap)	34-6
VLAN	vlan database	Console(config-vlan)	32-7
VDSL Line Profile	line-profile *profile-name*	Console(config-line-profile)	29-36
VDSL Alarm Profile	alarm-profile *profile-name*	Console(config-alarm-profile)	29-52
IGMP Profile	ip igmp profile *profile-number*	Console(config-igmp-profile)	35-16

Downloaded from www.Manualslib.com manuals search engine

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
⋮
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 18-3 Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.

Downloaded from www.Manualslib.com manuals search engine

Table 18-3 Keystroke Commands (Continued)

Keystroke	Function
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Table 18-4 Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	19-1
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, and the system clock	20-1
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	21-1
User Authentication	Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses	22-1
Client Security	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, filtering DHCP requests and replies, and filtering unwanted NetBIOS traffic	23-1
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code), or non-IP frames (based on MAC address or Ethernet type)	24-1

Downloaded from www.Manualslib.com manuals search engine

Table 18-4 Command Group Index (Continued)

Command Group	Description	Page
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	25-1
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	26-1
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	27-1
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	28-1
VDSL	Configures communication parameters for VDSL ports on the switch and connected CPEs	29-1
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	30-1
Spanning Tree	Configures Spanning Tree settings for the switch	31-1
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, and QinQ tunneling	32-1
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/ UDP traffic types, IP precedence, and DSCP	33-1
Quality of Service	Configures Differentiated Services	34-1
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration	35-1
Domain Name Service	Configures DNS services.	36-1
DHCP Client and Relay	Configures DHCP client and relay services (including DHCP Relay Option 82)	37-1
IP Interface	Configures IP address for the switch	38-1

Downloaded from www.Manualslib.com manuals search engine

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)
CM (Class Map Configuration)
NE (Normal Exec)
GC (Global Configuration)
IC (Interface Configuration)
IPC (IGMP Profile Configuraiton)
LC (Line Configuration)
MST (Multiple Spanning Tree)
PE (Privileged Exec)
PM (Policy Map Configuration)
VC (VLAN Database Configuration)
VLP (VDSL Line Profile)
VAP (VDSL Alarm Profile)

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 19
GENERAL COMMANDS

These commands are used to control the command access mode, configuration mode, and other basic functions.

Table 19-1 General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	19-2
disable	Returns to normal mode from privileged mode	PE	19-3
configure	Activates global configuration mode	PE	19-3
show history	Shows the command history buffer	NE, PE	19-4
reload	Restarts the system	PE	19-5
prompt	Customizes the CLI prompt	GC	19-6
end	Returns to Privileged Exec mode	any config. mode	19-6
exit	Returns to the previous configuration mode, or exits the CLI	any	19-7
quit	Exits a CLI session	NE, PE	19-7
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

Downloaded from www.Manualslib.com manuals search engine

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 18-7.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

"super" is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 22-4.)

The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable (19-3)
enable password (22-4)

Downloaded from www.Manualslib.com manuals search engine

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 18-7.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

enable (19-2)

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration. See "Understanding Command Modes" on page 18-7.

Default Setting

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#configure
Console(config)#
```

Related Commands

end (19-6)

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```


Downloaded from www.Manualslib.com manuals search engine

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

This command restarts the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```


Downloaded from www.Manualslib.com manuals search engine

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
```

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```


Downloaded from www.Manualslib.com manuals search engine

exit

This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 20
SYSTEM MANAGEMENT COMMANDS

These commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 20-1 System Management Commands

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	20-2
System Status	Displays system configuration, active managers, and version information	20-3
System Mode	Configures the switch to operate in normal mode, QinQ mode, or VLAN swap mode	20-13
Frame Size	Enables support for jumbo frames	20-15
File Management	Manages code image or ECN330-switch configuration files	20-16
Line	Sets communication parameters for the serial port, including baud rate and console time-out	20-26
Event Logging	Controls logging of error messages	20-39
SMTP Alerts	Configures SMTP email alerts	20-48
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually	20-53

Downloaded from www.Manualslib.com manuals search engine

Device Designation Commands

This section describes commands used to configure information that uniquely identifies the switch.

Table 20-2 Device Designation Commands

Command	Function	Mode	Page
hostname	Specifies the host name for the switch	GC	20-2
snmp-server contact	Sets the system contact string	GC	21-5
snmp-server location	Sets the system location string	GC	21-5

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname RD#1
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

System Status Commands

This section describes commands used to display system information.

Table 20-3 System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	20-3
show running-config	Displays the configuration data currently in use	PE	20-6
show system	Displays system information	NE, PE	20-8
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	20-9
show version	Displays version information for the system	NE, PE	20-10
show bme version	Displays version information for VDSL chip, BME, AFE, and IFE	PE	20-10
show cpu utilization	Shows CPU utilization parameters	NE, PE	20-11
show memory status	Shows memory utilization parameters	NE, PE	20-12

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Command Mode

Privileged Exec

Command Usage

Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.

Downloaded from www.Manualslib.com manuals search engine

This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

- MAC address for the switch
- SNTP server settings
- SNMP community strings
- Users (names and access levels)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address
- Layer 4 precedence settings
- Spanning tree settings
- Interface settings
- Any configured settings for the console port and Telnet

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show startup-config
building startup-config, please wait.....
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-20-1a-df-9c-a0_00</stackingMac>
!
phymap 00-20-1a-df-9c-a0
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community public ro
snmp-server community private rw
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree MST configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 lre channel interleave
lre psd-apply
:
interface vlan 1
 ip address dhcp
!
no map IP precedence
no map IP DSCP
!
line console
!
line VTY
!
end

Console#
```

Related Commands

show running-config (20-6)

Downloaded from www.Manualslib.com manuals search engine

show running-config

This command displays the configuration information currently in use.

Command Mode

Privileged Exec

Command Usage

Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.

This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

- MAC address for the switch
- SNTP server settings
- SNMP community strings
- Users (names, access levels, and encrypted passwords)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address
- Layer 4 precedence settings
- Spanning tree settings
- Interface settings
- Any configured settings for the console port and Telnet

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show running-config
building running-config, please wait.....
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-30-f1-d4-73-a0_00</stackingMac>
!
phymap 00-30-f1-d4-73-a0
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree MST-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 lre channel interleave
 lre datarate down fast  max 200000
 lre datarate down fast  min 64
 lre datarate down slow max 0
 lre datarate down slow min 0
 lre datarate up fast  max 200000
 lre datarate up fast  min 64
 lre datarate up slow max 0
 lre datarate up slow min 0
 lre psd-apply
:
interface vlan 1
 IP address DHCP
!
no map IP precedence
no map IP DSCP
!
line console
!
line vty
!
end

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

show startup-config (20-3)

show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to "Displaying System Information" on page 4-1.
- The POST results should all display "PASS." If any POST test indicates "FAIL," contact your distributor for assistance.

Example

```
Console#show system
System Description: TigerAccess(TM) SMC7816M/VSW
System OID String: 1.3.6.1.4.1.202.40.2
System information
 System Up time: 0 days, 1 hours, 23 minutes, and 44.61 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC Address (Unit1):     00-20-1A-DF-9C-A0
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled

 POST Result:
DUMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
PCI Device 1 Test ............ PASS
I2C Bus Initialization ....... PASS

Done All Pass.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None
     steve        15        RSA

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:14:14
* 1     VTY 0    admin           0:00:00    192.168.1.19
  2     SSH 1    steve           0:00:06    192.168.1.19

 Web online users:
  Line        Remote IP addr Username Idle time (h:m:s).
  ----------- -------------- -------- ------------------
 1      HTTP   192.168.1.19    admin           0:00:00

Console#
```


Downloaded from www.Manualslib.com manuals search engine

show version

This command displays hardware and software version information for the system.

Command Mode

Normal Exec, Privileged Exec

Command Usage

See "Displaying Hardware/Software Versions" on page 4-7 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit1
 Mainboard Serial Number:              A639000835
 Signalboard Serial Number:            A639000958
 Mainboard Hardware Version:           R01
 Signalboard Hardware Version:         R01
 EPLD1 Version:                        0.09
 EPLD2 Version:                        0.09
 Number of Ports:                      19
 Main Power Status:                    Up

Agent (Master)
 Unit ID:                  1
 Loader Version:           3.0.0.5
 Boot ROM Version:         3.2.1.0
 Operation Code Version:   3.2.2.5

 Bme firmware version:     Firmware-VTU-O:1.0.5r11IK004010

Console#
```

show bme version

This command displays version information for VDSL chip, Burst Mode Engine (BME), Analog Front End (AFE), and Integrated Front End (IFE).

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show bme version
Firmware            Firmware-VTU-O:1.0.5r11IK004010
Time                May 19 2006 18:16:42,
RTOS                Nucleus
BME                 R:96
AFE<num, ver>       <0:b10> <1:b10>
                    IFE<num:Dev.Rev> <0:3.6> <1:3.6> <2:3.6> <3:3.6>
                    <4:3.6> <5:3.6> <6:3.6> <7:3.6>
Console#
```

Table 20-4 show bme version - display description

Field	Description
Firmware	Primary application firmware version of VDSL chip
Time	Firmware compile time
RTOS	Name of Real-Time Operating System
BME	Burst Mode Engine (DSP) chip revision
AFE	Analog Front End (DA/AD converter) chip revision
IFE	Integrated Front End (Port VDSL filtering) chip revision

show cpu utilization

This command shows the CPU utilization parameters.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show cpu utilization

 CPU current utilization  : 73%
     Max utilization in 10s: 73%
     Avg utilization in 10s: 73%

     peak utilization: 73%
     peak utilization begin : 02:33:50 01/01/2001
     peak utilization during: 10(s)

     utilization Raise  threshold: 90%
     utilization Falling threshold: 70%
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Table 20-5 show cpu utilization - display description

Field	Description
current utilization	Current percentage of CPU utilization
max utilization	Maximum statistical utilization over the past 10 seconds
avg utilization	Average statistical utilization since the system was booted
peak utilization	Peak utilization over the indicated period
peak begin	Time at which the duration of peak utilization began
peak during	Duration of peak utilization
rising threshold*	Rising threshold for CPU utilization alarm
falling threshold*	Falling threshold for CPU utilization alarm

* For information on setting these thresholds, see "Displaying System Health" on page 4-4

show memory status

This command shows memory utilization parameters.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show memory status

FREE LIST:
  num     addr      size
  --- ---------- ----------
    1  0x7176640       1024
    2  0x7176498         56


SUMMARY:
 status   bytes    blocks   avg block  max block
 ------ --------- -------- ---------- ----------
current
   free      1080        2        540       1024
  alloc   8984600    46724        192          -
cumulative
  alloc  21630136   156917        137          -

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Table 20-6 show memory status - display description

Field	Description
free list	The location and size of free system memory
current	
free	Amount of memory currently free for use
allocated	Amount of memory allocated to active processes
cumulative	
allocated	Amount of memory allocated since the system was booted

System Mode Commands

This section describes command used to configure the switch to operate in normal mode or QinQ mode.

Table 20-7 System Mode Commands

Command	Function	Mode	Page
system mode	Configures the switch to operate in normal mode, QinQ mode, or VLAN-swap mode	GC	20-13
show system mode	Displays the switch system mode	GC	20-14

system mode

This command sets the switch to operate in QinQ mode. Use the **no** form to restore the default setting of normal operating mode.

Syntax

system mode {**normal** | **qinq** | **vlan-swap**}
no system mode

- **normal** – Sets the switch to normal operating mode.
- **qinq** – Sets the switch to QinQ mode, and allows the dot1q tunnel port to be configured. For an explanation of QinQ, see "Configuring IEEE 802.1Q Tunneling" on page 32-25.
- **vlan-swap** – Sets the switch to VLAN Swap mode. For an explanation of this feature, see "Configuring VLAN Swapping" on page 32-30.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Normal operating mode

Command Mode

Global Configuration

Command Usage

Make sure that no dot1q-tunnel port is configured before exiting QinQ mode (see "switchport mode dot1q-tunnel" on page 32-27). If there are any dot1q-tunnel ports set on the switch, the **no system mode** command will fail.

Example

```
Console(config)#system mode qinq
Console(config)#
```

Related Commands

show system mode (20-14)

show system mode

This command displays the switch system mode.

Command Mode

Privileged Exec

Command Usage

The system mode displays as QinQ or Normal mode.

Example

```
Console(config)#system mode qinq
Console(config)#end
Console#show system mode
system mode:qinq
Console#
```

Related Commands

system mode (20-13)

Downloaded from www.Manualslib.com manuals search engine

Frame Size Commands

This section describes commands used to configure the Ethernet frame size on the switch.

Table 20-8 Frame Size Commands

Command	Function	Mode	Page
jumbo frame	Enables support for jumbo frames	GC	20-15

jumbo frame

This command enables support for jumbo frames for Gigabit Ethernet ports. Use the **no** form to disable it.

Syntax

[**no**] **jumbo frame**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- The current setting for jumbo frames can be displayed with the **show system** command (page 20-8).

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#jumbo frame
Console(config)#
```

File Management Commands

Managing Firmware

Firmware can be uploaded and downloaded to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from a TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Table 20-9 Flash/File Commands

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	20-17
delete	Deletes a file or code image	PE	20-22
dir	Displays a list of files in flash memory	PE	20-23

Downloaded from www.Manualslib.com manuals search engine

Table 20-9 Flash/File Commands (Continued)

Command	Function	Mode	Page
whichboot	Displays the files booted	PE	20-24
boot system	Specifies the file or image used to start up the system	GC	20-25

copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** |
https-certificate | **public-key** | **firmware**}
copy partial-running-config startup-configfile

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Keyword that allows you to copy the HTTPS secure site certificate.
- **public-key** - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell Commands" on page 22-21.)
- **partial-running-config** - Keyword that allows you to copy the IP address, subnet mask, default gateway, SNMP community strings, CLI user names and passwords to a configuration file. All other

Downloaded from www.Manualslib.com manuals search engine

settings will be set to default values when the system is rebooted using this file.

- **firmware** - Keyword that allows you to copy BME firmware used for upgrading CPEs to reserved buffer space in the switch. (BME indicates the Burst Mode Engine used for digital signal processing.)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" on page 6-9. For information on configuring the switch to use HTTPS for a secure connection, see "ip http secure-server" on page 22-17.

Downloaded from www.Manualslib.com manuals search engine

- Use the **partial-running-config** keyword to copy basic settings for the IP configuration, SNMP community strings, and CLI user names and passwords to a startup configuration file. The system can then be reset using the parameters copied from the partial-running-config, and default settings for all other parameters.
- After using the **firmware** keyword to copy BME firmware for CPEs to reserved buffer space in the switch, first use the **oam remote upgrade firmware** command (page x) to transfer the firmware a remote CPE, and then use the oam remote firmware active command (page x) to activate the new firmware.

Example

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: LUVDSL2_Opcode_V3.1.16.20.bix
Destination file name: V311620
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```


Downloaded from www.Manualslib.com manuals search engine

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```


Downloaded from www.Manualslib.com manuals search engine

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

This example shows how to copy BME firmware for CPEs to a reserved buffer on the switch, copy this firmware to a remote CPE, and then activate the new firmware. For more detailed information on these commands, refer to the **copy tftp firmware**, **oam remote upgrade firmware**, and **oam remote firmware active** (page 29-87, 29-90 and page 29-90).

```
Console#copy tftp firmware
TFTP server IP address: 192.168.1.19
Source file name: 724maccpe
Success.
Firmware size :         485719
Firmware version :      104012IK7.2.4r9_Back_to_Back_Mac
Console#configure
Console(config)#interface ethernet 1/16
Console(config-if)#oam remote upgrade firmware
Console(config-if)#oam remote firmware active
port 1/16:      Success to active remote firmware
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

delete

This command deletes a file or image.

Syntax

delete *filename*

filename - Name of configuration file or code image.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- "Factory_Default_Config.cfg" cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (20-23)
delete public-key (22-28)

Downloaded from www.Manualslib.com manuals search engine

dir

This command displays a list of files in flash memory.

Syntax

dir {{**boot-rom:** | **config:** | **opcode:**} [*filename*]}

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

If you enter the command **dir** without any parameters, the system displays all files.

File information is shown below:

Table 20-10 File Directory Information

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to display all file information:

```
Console#dir
          File name                       File type       Startup Size (byte)
 ------------------------------------     --------------  ------- -----------
 Unit1:
          SMC7816M_VSW_Diag_V3.2.1.0.bix   Boot-Rom Image  Y          1556680
          SMC7816M_VSW_Opcode_V3.2.2.5.bix Operation Code  Y          4250428
          Factory_Default_Config.cfg       Config File     N              455
          startup1.cfg                     Config File     Y             2698
 ------------------------------------------------------------------------
                                                 Total free space:   9043968
Console#
```

whichboot

This command displays which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
          File name                       File type       Startup Size (byte)
 ------------------------------------     --------------  ------- -----------
 Unit1:
          SMC7816M_VSW_Diag_V3.2.1.0.bix   Boot-Rom Image  Y          1556680
          SMC7816M_VSW_Opcode_V3.2.2.5.bix Operation Code  Y          4250428
          Factory_Default_Config.cfg       Config File     N              455
          startup1.cfg                     Config File     Y             2698
 ------------------------------------------------------------------------
                                                 Total free space:   9043968
Console#
```


Downloaded from www.Manualslib.com manuals search engine

boot system

This command specifies the file or image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom*** - Boot ROM.
- **config*** - Configuration file.
- **opcode*** - Run-time operation code.
- *filename* - Name of configuration file or code image.

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

A colon (:) is required after the specified file type.

If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (20-23)
whichboot (20-24)

Downloaded from www.Manualslib.com manuals search engine

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 20-11 Line Commands

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	20-27
login	Enables password checking at login	LC	20-28
password	Specifies a password on a line	LC	20-29
timeout login response	Sets the interval that the system waits for a login attempt	LC	20-30
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	20-31
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	20-32
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	20-33
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	20-33
parity*	Defines the generation of a parity bit	LC	20-34
speed*	Sets the terminal baud rate	LC	20-35
stopbits*	Sets the number of the stop bits transmitted per byte	LC	20-36
disconnect	Terminates a line connection	PE	20-36
show line	Displays a terminal line's parameters	NE, PE	20-37

* These commands only apply to the serial port.

Downloaded from www.Manualslib.com manuals search engine

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as "VTY" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (20-37)
show users (20-9)

Downloaded from www.Manualslib.com manuals search engine

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (22-2)
password (20-29)

password

This command specifies the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the

Downloaded from www.Manualslib.com manuals search engine

configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (20-28)
password-thresh (20-32)

timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

Syntax

timeout login response [*seconds*]
no timeout login response

seconds - Integer that specifies the timeout interval. (Range: 0 - 300 seconds; 0: disabled)

Default Setting

CLI: Disabled (0 seconds)
Telnet: 300 seconds

Command Mode

Line Configuration

Command Usage

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Downloaded from www.Manualslib.com manuals search engine

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]
no exec-timeout

seconds - Integer that specifies the timeout interval.
(Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```


Downloaded from www.Manualslib.com manuals search engine

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]
no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (20-33)

Downloaded from www.Manualslib.com manuals search engine

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration (console only)

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (20-32)

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (20-34)

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default Setting

auto

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the "auto" option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Downloaded from www.Manualslib.com manuals search engine

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

Specifying session identifier "0" will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

show ssh (22-31)
show users (20-9)

show line

This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout: Disabled
  Silent time:         Disabled
  Baudrate:            auto
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Event Logging Commands

This section describes commands used to configure event logging on the switch.

Table 20-12 Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	20-39
logging history	Limits syslog messages saved to switch memory based on severity	GC	20-40
logging host	Adds a syslog server host IP address that will receive logging messages	GC	20-41
logging facility	Sets the facility type for remote logging of syslog messages	GC	20-42
logging trap	Limits syslog messages saved to a remote server based on severity	GC	20-43
clear log	Clears messages from the logging buffer	PE	20-44
show logging	Displays the state of logging	PE	20-45
show log	Displays log messages	PE	20-47

logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

[**no**] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the **logging history**

Downloaded from www.Manualslib.com manuals search engine

command to control the type of error messages that are stored in memory. You can use the **logging trap** command to control the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (20-40)
logging trap (20-43)
clear log (20-44)

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 20-13 Logging Levels

Level	Severity Name	Description
7	debugging	Debugging messages
6	informational	Informational messages only
5	notifications	Normal but significant condition, such as cold start

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Downloaded from www.Manualslib.com manuals search engine

Table 20-13 Logging Levels (Continued)

Level	Severity Name	Description
4	warnings	Warning conditions (e.g., return false, unexpected return)
3	errors	Error conditions (e.g., invalid input, default used)
2	critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	alerts	Immediate action needed
0	emergencies	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

[**no**] **logging host** *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

- Use this command more than once to build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

[**no**] **logging facility** *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

Syntax

logging trap [*level*]
no logging trap

level - One of the syslog severity levels listed in the table on page 20-40. Messages sent include the selected level up through level 0.

Default Setting

Disabled

Level 7 - 0

Command Mode

Global Configuration

Command Usage

Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.

Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

Example

```
Console(config)#logging trap 4
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

clear log

This command clears messages from the log buffer.

Syntax

clear log [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear log
Console#
```

Related Commands

show log (20-47)

Downloaded from www.Manualslib.com manuals search engine

show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

show logging {**flash** | **ram** | **sendmail** | **trap**}

- **flash** - Displays settings for storing event messages in flash memory (i.e., permanent memory).
- **ram** - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).
- **sendmail** - Displays settings for the SMTP event handler (page 20-52).
- **trap** - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), and the message level for RAM is "debugging" (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
Console#
```

Table 20-14 show logging flash/ram - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
History logging in FLASH	The message level(s) reported based on the **logging history** command.
History logging in RAM	The message level(s) reported based on the **logging history** command.

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type:        Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

Table 20-15 show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
REMOTELOG status	Shows if remote logging has been enabled via the **logging trap** command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the **logging facility** command.

Downloaded from www.Manualslib.com manuals search engine

Table 20-15 show logging trap - display description (Continued)

Field	Description
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the **logging trap** command.
REMOTELOG server IP address	The address of syslog servers as specified in the **logging host** command.

Related Commands

show logging sendmail (20-52)

show log

This command displays the log messages stored in local memory.

Syntax

show log {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```


Downloaded from www.Manualslib.com manuals search engine

SMTP Alert Commands

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 20-16 SMTP Alert Commands

Command	Function	Mode	Page
logging sendmail host	SMTP servers to receive alert messages	GC	20-48
logging sendmail level	Severity threshold used to trigger alert messages	GC	20-49
logging sendmail source-email	Email address used for "From" field of alert messages	GC	20-50
logging sendmail destination-email	Email recipients of alert messages	GC	20-50
logging sendmail	Enables SMTP event handling	GC	20-51
show logging sendmail	Displays SMTP event handler settings	NE, PE	20-52

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[**no**] **logging sendmail host** *ip_address*

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.

Downloaded from www.Manualslib.com manuals search engine

- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level *level*

level - One of the system message levels (page 20-40). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

logging sendmail source-email

This command sets the email address used for the "From" field in alert messages.

Syntax

logging sendmail source-email *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email
  ted@this-company.com
Console(config)#
```

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[**no**] **logging sendmail**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
192.168.1.19

SMTP minimum severity level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 20-17 Time Commands

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	20-53
sntp server	Specifies one or more time servers	GC	20-54
sntp poll	Sets the interval at which the client polls for time	GC	20-55
show sntp	Shows current SNTP configuration settings	NE, PE	20-56
clock timezone	Sets the time zone for the switch's internal clock	GC	20-57
calendar set	Sets the system date and time	PE	20-58
show calendar	Displays the current date and time setting	NE, PE	20-58

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form to disable SNTP client requests.

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

Related Commands

sntp server (20-54)
sntp poll (20-55)
show sntp (20-56)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (20-53)
sntp poll (20-55)
show sntp (20-56)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*
no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Example

```
Console(config)#sntp poll 60
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

sntp client (20-53)

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```


Downloaded from www.Manualslib.com manuals search engine

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 0-13 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (20-56)

Downloaded from www.Manualslib.com manuals search engine

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit). (Range: 2001 - 2100)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show calendar
 15:12:34 February 1 2002
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 21
SNMP COMMANDS

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 21-1 SNMP Commands

Command	Function	Mode	Page
snmp-server	Enables the SNMP agent	GC	21-2
show snmp	Displays the status of SNMP communications	NE, PE	21-3
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	21-4
snmp-server contact	Sets the system contact string	GC	21-5
snmp-server location	Sets the system location string	GC	21-5
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	21-6
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	21-9
rate-limit trap-input	Sets an SNMP trap if traffic exceeds the configured rate limit	IC	28-3

Downloaded from www.Manualslib.com manuals search engine

Table 21-1 SNMP Commands (Continued)

Command	Function	Mode	Page
snmp-server engine-id	Sets the SNMP engine ID	GC	21-10
show snmp engine-id	Shows the SNMP engine ID	PE	21-12
snmp-server view	Adds an SNMP view	GC	21-13
show snmp view	Shows the SNMP views	PE	21-14
snmp-server group	Adds an SNMP group, mapping users to views	GC	21-15
show snmp group	Shows the SNMP groups	PE	21-16
snmp-server user	Adds a user to an SNMP group	GC	21-18
show snmp user	Shows the SNMP users	PE	21-20

snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[**no**] **snmp-server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

show snmp

This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP Agent: enabled

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

snmp-server community

This command defines the SNMP v1 and v2c community access string. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (21-5)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (21-5)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]] *community-string* [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- **inform** - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - *retries* - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
  - *seconds* - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- *community-string* - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server**

Downloaded from www.Manualslib.com manuals search engine

community command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

- **version** - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)
  - **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 5-1 for further information about these authentication and encryption options.
- *port* - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

Host Address: None
Notification Type: Traps
SNMP Version: 1
UDP Port: 162

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.

Downloaded from www.Manualslib.com manuals search engine

- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 21-2).
  2. Allow the switch to send SNMP traps; i.e., notifications (page 21-9).
  3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
  4. Create a view with the required notification messages (page 21-13).
  5. Create a group that includes the required notify view (page 21-15).

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 21-2).
  2. Allow the switch to send SNMP traps; i.e., notifications (page 21-9).
  3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
  4. Create a view with the required notification messages (page 21-13).
  5. Create a group that includes the required notify view (page 21-15).
  6. Specify a remote engine ID where the user resides (page 21-10).
  7. Then configure a remote user (page 21-18).

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. If you use the V3 "auth" or "priv" options, the user name must first be defined with the **snmp-server**

Downloaded from www.Manualslib.com manuals search engine

user command. Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the "noauth" option, an SNMP user account will be generated, and the switch will authorize SNMP access for the host.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (21-9)

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure notifications.
- **link-up-down** - Keyword to issue link-up or link-down notifications.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down

Downloaded from www.Manualslib.com manuals search engine

notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command (page 21-15).

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (21-6)

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*
no snmp-server engine-id {**local** | **remote** {*ip-address*}}

- **local** - Specifies the SNMP engine on this switch.
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- *engineid-string* - String identifying the engine ID.
  (Range: 1-26 hexadecimal characters for the local engine ID and 10-64 for a remote engine ID)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Command Usage

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See **snmp-server host** on page 21-6.) The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.
- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID or 54 zeroes for a remote engine ID.
- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 21-18).

Example

```
Console(config)#snmp-server engine-id local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#
```

Related Commands

snmp-server host (21-6)

Downloaded from www.Manualslib.com manuals search engine

show snmp engine-id

This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                        IP address
80000000030004e2b316c54321                                  192.168.1.19
Console#
```

Table 21-2 show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

Downloaded from www.Manualslib.com manuals search engine

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

- *view-name* - Name of an SNMP view. (Range: 1-64 characters)
- *oid-tree* - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)
- **included** - Defines an included view.
- **excluded** - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- Views are used in the **snmp-server group** command to restrict user access to specified portions of the MIB tree.
- The predefined view "defaultview" includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
  included
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
included
Console(config)#
```

show snmp view

This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

Console#
```

Table 21-3 show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

Downloaded from www.Manualslib.com manuals search engine

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]
no snmp-server group *groupname*

- *groupname* - Name of an SNMP group. (Range: 1-32 characters)
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 5-1 for further information about these authentication and encryption options.
- *readview* - Defines the view for read access. (1-64 characters)
- *writeview* - Defines the view for write access. (1-64 characters)
- *notifyview* - Defines the view for notifications. (1-64 characters)

Default Setting

Default groups: public[27] (read only), private[28] (read/write)
readview - Every object belonging to the Internet OID space (1.3.6.1).
writeview - Nothing is defined.
notifyview - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the snmp-server user command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.

27. No view is defined.
28. Maps to the defaultview.

Downloaded from www.Manualslib.com manuals search engine

- For additional information on the notification messages supported by this switch, see Table 5-2, "Supported Notification Messages," on page 5-19. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the **snmp-server enable traps** command (page 21-9).

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
```


Downloaded from www.Manualslib.com manuals search engine

```
Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

Table 21-4 show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

Downloaded from www.Manualslib.com manuals search engine

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

- *username* - Name of user connecting to the SNMP agent. (Range: 1-32 characters)
- *groupname* - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **encrypted** - Accepts the password as encrypted input.
- **auth** - Uses SNMPv3 with authentication.
- **md5** | **sha** - Uses MD5 or SHA authentication.
- *auth-password* - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)
- **priv des56** - Uses SNMPv3 with privacy with DES56 encryption.
- *priv-password* - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the **snmp-server engine-id** command before using this configuration command.
- Before you configure a remote user, use the **snmp-server engine-id** command (page 21-10) to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve group r&d v3 auth md5
  greenpeace priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19
  v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

show snmp user

This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 21-5 show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 22
USER AUTHENTICATION COMMANDS

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access[29] to the data ports.

Table 22-1 Authentication Commands

Command Group	Function	Page
User Accounts	Configures the basic user names and passwords for management access	22-2
Authentication Sequence	Defines logon authentication method and precedence	22-5
RADIUS Client	Configures settings for authentication via a RADIUS server	22-8
TACACS+ Client	Configures settings for authentication via a TACACS+ server	22-13
Web Server Settings	Enables management access via a web browser	22-15
Telnet Server Settings	Enables management access via Telnet	22-20
Secure Shell Settings	Provides secure replacement for Telnet	22-21
Port Authentication	Configures host authentication on specific ports using 802.1X	22-34
Management IP Filter	Configures IP addresses that are allowed management access	22-45

29. For other methods of controlling client access, see "Client Security Commands" on page 23-1.

Downloaded from www.Manualslib.com manuals search engine

User Account Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 20-26), user authentication via a remote authentication server (page 22-1), and host access authentication for specific ports (page 22-34).

Table 22-2 User Access Commands

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	22-2
enable password	Sets a password to control access to the Privileged Exec level	GC	22-4

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}
no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
  The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.

Downloaded from www.Manualslib.com manuals search engine

- **password** *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

The default access level is Normal Exec.

The factory defaults for the user names and passwords are:

Table 22-3 Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.

(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

The default is level 15.
The default password is "super"

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 19-2).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

enable (19-2)
authentication enable (22-7)

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 22-4 Authentication Sequence Commands

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	22-5
authentication enable	Defines the authentication method and precedence for command mode change	GC	22-7

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local password.
- **radius** - Use RADIUS server password.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (22-2)

Downloaded from www.Manualslib.com manuals search engine

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command (see page 19-2). Use the **no** form to restore the default.

Syntax

authentication enable {[**local**] [**radius**] [**tacacs**]}
no authentication enable

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

enable password - sets the password for changing command modes (22-4)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 22-5 RADIUS Client Commands

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	22-9
radius-server port	Sets the RADIUS server network port	GC	22-10
radius-server key	Sets the RADIUS encryption key	GC	22-10
radius-server retransmit	Sets the number of retries	GC	22-11
radius-server timeout	Sets the interval between sending authentication requests	GC	22-11
show radius-server	Shows the current RADIUS settings	PE	22-12

Downloaded from www.Manualslib.com manuals search engine

radius-server host

This command specifies primary and backup RADIUS servers and authentication parameters that apply to each server. Use the **no** form to restore the default values.

Syntax

[**no**] **radius-server** *index* **host** {*host_ip_address* | *host_alias*} [**auth-port** *auth_port*] [**timeout** *timeout*] [**retransmit** *retransmit*] [**key** *key*]

- *index* - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.
- *host_ip_address* - IP address of server.
- *host_alias* - Symbolic name of server. (Maximum length: 20 characters)
- *port_number* - RADIUS server UDP port used for authentication messages. (Range: 1-65535)
- *timeout* - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)
- *retransmit* - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)
- *key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Setting

auth-port - 1812
timeout - 5 seconds
retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout
  10 retransmit 5 key green
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   1812
 Retransmit times:                     2
 Request timeout:                      5

Server 1:
 Server IP address:                    192.168.1.1
 Communication key with RADIUS server: *****
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5

Console#
```


Downloaded from www.Manualslib.com manuals search engine

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 22-6 TACACS+ Client Commands

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	22-13
tacacs-server port	Specifies the TACACS+ server network port	GC	22-14
tacacs-server key	Sets the TACACS+ encryption key	GC	22-14
show tacacs-server	Shows the current TACACS+ settings	GC	22-15

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address:                    10.11.12.13
 Communication key with TACACS server: *****
 Server port number:                   49
Console#
```

Web Server Commands

This section describes commands used to configure web browser management access to the switch.

Table 22-7 Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the web browser interface	GC	22-16
ip http server	Allows the switch to be monitored or configured from a browser	GC	22-16
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC	22-17
ip http secure-port	Specifies the UDP port number for HTTPS	GC	22-18

Downloaded from www.Manualslib.com manuals search engine

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (22-16)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[**no**] **ip http server**

Default Setting

Enabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (22-16)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.

Downloaded from www.Manualslib.com manuals search engine

- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 6.2 or later versions.
- The following web browsers and operating systems currently support HTTPS:

Table 22-8 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 6-9. Also refer to the **copy** command on page 20-17.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (22-18)
copy tftp https-certificate (20-17)

ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS. (Range: 1-65535)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (22-17)

Downloaded from www.Manualslib.com manuals search engine

Telnet Server Commands

This section describes commands used to configure Telnet management access to the switch.

Table 22-9 Telnet Server Commands

Command	Function	Mode	Page
ip telnet server	Allows the switch to be monitored or configured from Telnet; also specifies the port to be used by the Telnet interface	GC	22-16

ip telnet server

This command allows this device to be monitored or configured from Telnet. It also specifies the TCP port number used by the Telnet interface. Use the **no** form without the "port" keyword to disable this function. Use the **no** from with the "port" keyword to use the default port.

Syntax

ip telnet server [**port** *port-number*]
no telnet server [**port**]

- **port** - The TCP port used by the Telnet interface.
- *port-number* - The TCP port number to be used by the browser interface. (Range: 1-65535)

Default Setting

Server: Enabled
Server Port: 23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#ip telnet port 123
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Secure Shell Commands

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 22-10 Secure Shell Commands

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	22-25
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	22-26
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	22-27
ip ssh server-key size	Sets the SSH server key size	GC	22-27
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE	20-17
delete public-key	Deletes the public key for the specified user	PE	22-28
ip ssh crypto host-key generate	Generates the host key	PE	22-28
ip ssh crypto zeroize	Clear the host key from RAM	PE	22-29
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	22-30
disconnect	Terminates a line connection	PE	20-36
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	22-31
show ssh	Displays the status of current SSH sessions	PE	22-31
show public-key	Shows the public key for the specified user or for the host	PE	22-32
show users	Shows SSH users, including privilege level and public key type	PE	20-9

Downloaded from www.Manualslib.com manuals search engine

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 22-5. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.
2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761171

3. Import Client's Public Key to the Switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the **username** command as described on page 22-2.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

Downloaded from www.Manualslib.com manuals search engine

1024 35 134108168560989392104094492015542534763164192187295892114317388005555361616310517759408386863110929123222682851925437460310093718772119969631781366277414168985132049117204830339254324101637997592371449011938006090253948408482717819437228840253311595213486102290297898272135326713162943253281891504530639391664 3 steve@192.168.1.19

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the switch.
6. Authentication – One of the following authentication methods is employed:

Password Authentication (for SSH v1.5 or V2 Clients)

a. The client sends its password to the server.

b. The switch compares the client's password to those stored in memory.

c. If a match is found, the connection is allowed.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.

b. The switch compares the client's public key to those stored in memory.

Downloaded from www.Manualslib.com manuals search engine

c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.

d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.

e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.

b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

c. The client sends a signature generated using the private key to the switch.

d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Downloaded from www.Manualslib.com manuals search engine

ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

[**no**] **ip ssh server**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate DSA and RSA host keys before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (22-28)
show ssh (22-31)

Downloaded from www.Manualslib.com manuals search engine

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (20-31)
show ip ssh (22-31)

Downloaded from www.Manualslib.com manuals search engine

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (22-31)

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*
no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

The server key is a private key that is never shared outside the switch. The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

This command deletes the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

- *username* – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** – DSA (Version 2) key type.
- **rsa** – RSA (Version 1) key type.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- This command stores the host key pair in memory (i.e., RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

ip ssh crypto zeroize (22-29)
ip ssh save host-key (22-30)

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (22-28)
ip ssh save host-key (22-30)
no ip ssh server (22-25)

ip ssh save host-key

This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (22-28)

Downloaded from www.Manualslib.com manuals search engine

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show ssh

This command displays the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5

Console#
```

Table 22-11 show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)

Downloaded from www.Manualslib.com manuals search engine

Table 22-11 show ssh - display description (Continued)

Field	Description
Username	The user name of the client.
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5 *Terminology:* DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

show public-key

This command shows the public key for the specified user or for the host.

Syntax

show public-key [**user** [*username*] | **host**]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 65537
13236940658254764031382795526536375927835525327972629521130241
07194210616557594245909392360969540503627752575562510038661309893933
83452310332802149888661921595568598879891919505883940181387440468908
87791603058377681854900028313416250083487184495220874292122556916656
65529632816351696404083155476606641516571163 81
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2Hxc YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1
N2XFfAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBr
RAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8
cZvH+/p9cnrfwFTMU01VFDly3IR 2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oG
CstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6BmiFq7O+jAhf1Dg45loAc27s6TLdtny1
wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXK
VYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2o/dVzX4Gg+yqdTl
YmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7 w0W
Console#
```


Downloaded from www.Manualslib.com manuals search engine

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 22-12 802.1X Port Authentication Commands

Command	Function	Mode	Page
dot1x system-auth-control	Enables dot1x globally on the switch.	GC	22-35
dot1x default	Resets all dot1x parameters to their default values	GC	22-35
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC	22-36
dot1x port-control	Sets dot1x mode for a port interface	IC	22-36
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC	22-37
dot1x re-authenticate	Forces re-authentication on specific ports	PE	22-38
dot1x re-authentication	Enables re-authentication for all ports	IC	22-39
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC	22-39
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC	22-40

Downloaded from www.Manualslib.com manuals search engine

Table 22-12 802.1X Port Authentication Commands (Continued)

Command	Function	Mode	Page
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC	22-41
show dot1x	Shows all dot1x related information	PE	22-41

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[**no**] **dot1x system-auth-control**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control
Console(config)#
```

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Downloaded from www.Manualslib.com manuals search engine

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*]}
no dot1x operation-mode [**multi-host max-count**]

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple host to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
  - *count* – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- The "max-count" parameter specified by this command is only effective if the dot1x mode is set to "auto" by the dot1x port-control command (page 4-105).

Downloaded from www.Manualslib.com manuals search engine

- In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

ethernet *unit/port*
- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-19)

Command Mode

Privileged Exec

Command Usage

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

Example

```
Console#dot1x re-authenticate
Console#
```


Downloaded from www.Manualslib.com manuals search engine

dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

[**no**] **dot1x re-authentication**

Command Mode

Interface Configuration

Command Usage

- The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

Related Commands

dot1x timeout re-authperiod (22-40)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Downloaded from www.Manualslib.com manuals search engine

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*
no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

- **statistics** - Displays dot1x status for each port.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch.
- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
  - Status – Administrative state for port access control.
  - Operation Mode – Allows single or multiple hosts (page 22-37).
  - Mode – Dot1x port control mode (page 22-36).
  - Authorized – Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
  - reauth-enabled – Periodic re-authentication (page 22-39).
  - reauth-period – Time after which a connected client must be re-authenticated (page 22-40).
  - quiet-period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 22-39).
  - tx-period – Time a port waits during authentication session before re-transmitting EAP packet (page 22-41).
  - supplicant-timeout – Supplicant timeout.
  - server-timeout – Server timeout.
  - reauth-max – Maximum number of reauthentication attempts.
  - max-req – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 22-36).
  - Status – Authorization status (authorized or not).
  - Operation Mode – Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
  - Max Count – The maximum number of hosts allowed to access this port (page 22-37).

Downloaded from www.Manualslib.com manuals search engine

- Port-control – Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 22-36).
- Supplicant – MAC address of authorized client.
- Current Identifier – The integer (0-255) used by the Authenticator to identify the current authentication session.

• *Authenticator State Machine*

- State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- Reauth Count – Number of times connecting state is re-entered.

• *Backend State Machine*

- State – Current state (including request, response, success, fail, timeout, idle, initialize).
- Request Count – Number of EAP Request packets sent to the Supplicant without receiving a response.
- Identifier(Server) – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

• *Reauthentication State Machine*

- State – Current state (including initialize, reauthenticate).

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show dot1x
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode              Authorized
1/1        disabled        Single-Host      ForceAuthorized     n/a
1/2        disabled        Single-Host      ForceAuthorized     n/a
:
1/17       disabled        Single-Host      ForceAuthorized     yes
1/18       enabled         Single-Host      Auto                yes

802.1X Port Details

802.1X is enabled on port 1/1
:
802.1X is enabled on port 18
reauth-enabled:       Enable
reauth-period:        3600
quiet-period:         60
tx-period:            30
supplicant-timeout:   30
server-timeout:       10
reauth-max:           2
max-req:              2
Status                Authorized
Operation mode        Multi-Host
Max count             5
Port-control          Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    3

Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Management IP Filter Commands

This section describes commands used to configure IP management access to the switch.

Table 22-13 Management IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	22-45
show management	Displays the switch to be monitored or configured from a browser	PE	22-46

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- *start-address* - A single IP address, or the starting address of a range.
- *end-address* - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 23
CLIENT SECURITY COMMANDS

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Private VLANs and port-based authentication using IEEE 802.1X are commonly used for these purposes. In addition to these methods, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses (either by freezing a set of dynamically learned entries or through static configuration), or to deny client access by statically configuring MAC/IP address pairs (using packet filtering rules). NetBIOS traffic commonly used for resource sharing in a peer-to-peer environment can be completely blocked to ensure that no privileged client data is passed to other data ports. DHCP service requests can also be blocked to ensure that only static addresses assigned by the service provider are used, or DHCP replies can be blocked on specific ports to ensure that DHCP service requests are only answered through authorized uplink ports. The addresses assigned to DHCP clients can also be carefully controlled using static or dynamic bindings with the IP Source Guard and DHCP Snooping commands.

Downloaded from www.Manualslib.com manuals search engine

Table 23-1 Client Security Commands

Command Group	Function	Page
Private VLANs	Configures private VLANs, including uplink and downlink ports	32-17
Port Authentication	Configures host authentication on specific ports using 802.1X	22-34
Port Security*	Configures secure addresses for a port	23-2
Packet Filtering*	Filters packets with specified IP/MAC addresses, NetBIOS packets, and DHCP requests or replies	23-5
IP Source Guard*	Filters IP traffic on unsecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings	23-11
DHCP Snooping*	Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table	23-17

* The priority of execution for these filtering commands is Port Security, Packet Filtering, IP Source Guard, and then DHCP Snooping.

Port Security Commands

These commands can be used to enable port security on a port. When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Downloaded from www.Manualslib.com manuals search engine

Table 23-2 Port Security Commands

Command	Function	Mode	Page
port security	Configures a secure port	IC	23-3
mac-address-table static	Maps a static address to a port in a VLAN	GC	30-2
show mac-address-table	Displays entries in the bridge-forwarding database	PE	30-4

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]
no port security [**action** | **max-mac-count**]

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable port.
- **max-mac-count**
  - *address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

Status: Disabled
Action: None
Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- If you enable port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port.
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- You can also manually add secure addresses with the **mac-address-table static** command.
- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown (25-10)
mac-address-table static (30-2)

Downloaded from www.Manualslib.com manuals search engine

Packet Filtering Commands

This section describes commands used to configure packet filtering for inbound traffic.

Table 23-3 Packet Filter Commands

Command	Function	Mode	Page
filter ipmac	Filters packets matching specified MAC address and IP address	GC	23-5
filter netbios	Filters NetBIOS packets	GC	23-7
filter dhcp-request	Filters DHCP request packets	GC	23-8
filter dhcp	Filters DHCP reply packets	GC	23-9
show filter	Displays packet filter settings	PE	23-10

Note: Packet Filtering occupies valuable hardware resources. Using Private VLANs provides a more efficient alternative for separating the traffic sent to each subscriber (see "Configuring Private VLANs" on page 32-17).

filter ipmac

This command filters packets matching the specified source MAC and IP address.

Syntax

filter ipmac add *interface MAC-address IP-address*
filter ipmac del *interface* [*MAC-address* [*IP-address*]]

- **add** - Adds a MAC and IP address pair to filter.
- **del** - Deletes all filtering entries, or an entry for a MAC and IP address pair.
- *interface*
  - *unit* - Stack unit. (Range: 1)
  - *port-list* - Single port number or list of ports. (Range: 1-18)
- *MAC-address* - Physical address of source.
- *IP-address* - IP address of source.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Both the specified source MAC address and source IP address for an entry must be matched to satisfy the filtering rule. Any packet matching a specified entry is dropped at the input port.
- To delete an entry for a MAC and IP address pair, you can specify either the MAC address or both the MAC and IP address.
- To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
- To specify a MAC address use either of the following hexidecimal formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. One mask is allocated to IP-MAC packet filtering if any entries are defined. This mask will be released for use by other filtering functions if all IP-MAC packet filtering entries are deleted.

Example

```
Console(config)#filter ipmac add 1/1 00-e0-29-94-34-de 192.168.0.33
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

filter netbios

This command filters NetBIOS[30] packets entering the specified input port.

Syntax

filter netbios {**add** | **del**} *interface*

- **add** - Enables NetBIOS filtering.
- **del** - Disables NetBIOS filtering.
- *interface*
  - *unit* - Stack unit. (Range: 1)
  - *port-list* - Single port number or list of ports. (Range: 1-18)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- NetBIOS is commonly used in local area networks to facilitate sharing resources such as printers or files between computers. However, when providing network services over the Internet to different customers, all information about local resources should be protected. Sending NetBIOS packets over TCP or UDP protocols can be manually disabled at the host computer. However, to ensure that this information is never sent out on the Internet, NetBIOS packet filtering should be enabled on all data ports if the switch is not operating behind a firewall.
- When NetBIOS packet filtering is enabled, NetBIOS packets addressed to any of the TCP or UDP ports 136-139 or 445, and carrying a DSAP[31] value of 0xE0 or 0xF0, will be dropped from the specified interface.
- To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.

30. NetBIOS - Network Basic Input Output System
31. DSAP - Destination Server Access Point; i.e., a session service tag

Downloaded from www.Manualslib.com manuals search engine

- This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. Three masks are allocated to NetBIOS packet filtering if enabled on any interface. These masks will be released for use by other filtering functions if NetBIOS packet filtering is disabled on all interfaces.

Example

```
Console(config)#filter netbios add 1/1
Console(config)#
```

filter dhcp-request

This command filters DHCP request packets.

Syntax

filter dhcp-request {**add** | **del**} *interface*

- **add** - Enables DHCP request filtering.
- **del** - Disables DHCP request filtering.
- *interface*
  - *unit* - Stack unit. (Range: 1)
  - *port-list* - Single port number or list of ports. (Range: 1-18)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- In cases where the IP address for a client attached to a downlink port is fixed (i.e., at the VDSL port on the CPE), you should use this command to block any DHCP requests from the client.
- To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
- This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. One mask is allocated to DHCP

Downloaded from www.Manualslib.com manuals search engine

packet filtering if enabled on any interface. This mask will be released for use by other filtering functions if DHCP packet filtering is disabled on all interfaces.

Example

```
Console(config)#filter dhcp-request add 1/1
Console(config)#
```

filter dhcp

This command filters DHCP reply packets.

Syntax

filter dhcp {**add** | **del**} *interface*

- **add** - Enables DHCP reply filtering.
- **del** - Disables DHCP reply filtering.
- *interface*
  - *unit* - Stack unit. (Range: 1)
  - *port-list* - Single port number or list of ports. (Range: 1-18)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- In cases where the client address is dynamically assigned by the service provider, but you need to ensure that the DHCP service reply is only obtained through an authorized uplink port, you can use this command to block DHCP replies from all unauthorized ports (commonly specifying all data ports).
- To specify a port list, use a hyphen to indicate a range of ports, or a comma to indicate a group of non-consecutive ports.
- This switch provides a total of 7 masks for filtering functions, including IP-MAC address packet filtering, NetBIOS packet filtering, DHCP packet filtering, and ACLs. One mask is allocated to DHCP packet filtering if enabled on any interface. This mask will be released

Downloaded from www.Manualslib.com manuals search engine

for use by other filtering functions if DHCP packet filtering is disabled on all interfaces.

Example

```
Console(config)#filter dhcp add 1/1
Console(config)#
```

show filter

This command displays the packet filter settings.

Command Mode

Privileged Exec

Example

```
Console#sh filter
PORT   DHCP[request]        DHCP[reply]  NetBIOS
1      restricted           restricted   restricted
2      free                 free         free
3      free                 free         free
4      free                 free         free
5      free                 free         free
6      free                 free         free
7      free                 free         free
8      free                 free         free
9      free                 free         free
10     free                 free         free
11     free                 free         free
12     free                 free         free
13     free                 free         free
14     free                 free         free
15     free                 free         free
16     free                 free         free
17     free                 free         free
18     free                 free         free
PORT   MAC Address          IP Address
1      00-e0-29-94-34-de    192.168.0.33
Console#
```


Downloaded from www.Manualslib.com manuals search engine

IP Source Guard Commands

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or static and dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping Commands" on page 23-17). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

Table 23-4 IP Source Guard Commands

Command	Function	Mode	Page
ip source-guard	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC	23-11
ip source-guard binding	Adds a static address to the source-guard binding table	GC	23-14
show ip source-guard	Shows whether source guard is enabled or disabled on each interface	PE	23-15
show ip source-guard binding	Shows the source guard binding table	PE	23-16

ip source-guard

This command configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

Syntax

ip source-guard {**sip** | **sip-mac**}
no ip source-guard

- **sip** - Filters traffic based on IP addresses stored in the binding table.
- **sip-mac** - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Source guard is used to filter traffic on an unsecure port which receives messages from outside the network or firewall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- Setting source guard mode to "sip" or "sip-mac" enables this function on the selected port. Use the "sip" option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the "sip-mac" option to check these same parameters, plus the source MAC address. Use the **no source guard** command to disable this function on the selected port.
- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.
- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, Static-DHCP-Binding), VLAN identifier, and port identifier.
- Static addresses entered in the source guard binding table with the **ip source-guard binding** command (page 23-14) are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself; static entries include a manually configured lease time.
- If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:
  - If the DHCP snooping is disabled (see page 23-18), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is

Downloaded from www.Manualslib.com manuals search engine

found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

- If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, static DHCP snooping binding or dynamic DHCP snooping binding, the packet will be forwarded.
- If IP source guard if enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.

Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

Related Commands

ip source-guard binding (23-14)
ip dhcp snooping (23-18)
ip dhcp snooping vlan (23-20)

Downloaded from www.Manualslib.com manuals search engine

ip source-guard binding

This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

Syntax

ip source-guard binding *mac-address* **vlan** *vlan-id ip-address*
interface ethernet *unit/port*
no ip source-guard binding *mac-address* **vlan** *vlan-id*

- *mac-address* - A valid unicast MAC address.
- *vlan-id* - ID of a configured VLAN (Range: 1-4093)
- *ip-address* - A valid unicast IP address, including classful types A, B or C.
- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-48)

Default Setting

No configured entries

Command Mode

Global Configuration

Command Usage

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, Static-DHCP-Binding), VLAN identifier, and port identifier.
- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the **show ip source-guard** command (page 23-15).
- When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.
- Static bindings are processed as follows:
  - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.

Downloaded from www.Manualslib.com manuals search engine

- If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
- If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Example

This example configures a static source-guard binding on port 5.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1
 192.168.0.99 interface ethernet 1/5
Console(config)#
```

Related Commands

ip source-guard (23-11)
ip dhcp snooping (23-18)
ip dhcp snooping vlan (23-20)

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard
Interface   Filter-type
---------   -----------
Eth 1/1     DISABLED
Eth 1/2     DISABLED
Eth 1/3     DISABLED
Eth 1/4     DISABLED
Eth 1/5     SIP
Eth 1/6     DISABLED
:
```


Downloaded from www.Manualslib.com manuals search engine

show ip source-guard binding

This command shows the source guard binding table.

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard binding
MacAddress        IpAddress       Lease(sec) Type                VLAN
Interface
----------------- --------------- ---------- -------------------- ---- --------
11-22-33-44-55-66 192.168.0.99             0 Static-IP-SG-binding    1 Eth 1/5
Console#
```


Downloaded from www.Manualslib.com manuals search engine

DHCP Snooping Commands

DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCP snooping.

Table 23-5 DHCP Snooping Commands

Command	Function	Mode	Page
ip dhcp snooping	Enables DHCP snooping globally	GC	23-18
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLAN	GC	23-20
ip dhcp snooping verify mac-address	Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC	23-21
ip dhcp snooping database write	Writes all dynamically learned snooping entries to flash memory	GC	23-22
ip dhcp snooping service-provider-mode	Converts the IP address assigned to a host by a DHCP server to a static entry, and registers the host as a valid entry in the DHCP snooping table	GC	23-22
ip dhcp snooping client limit	Limits the number of host devices which can be attached to a VDSL port	IC	23-23
ip dhcp snooping trust	Configures the specified interface as trusted	IC	23-24
show ip dhcp snooping	Shows the DHCP snooping configuration settings	PE	23-25
show ip dhcp snooping binding	Shows the DHCP snooping binding table entries	PE	23-26

Downloaded from www.Manualslib.com manuals search engine

ip dhcp snooping

This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

Syntax

[**no**] **ip dhcp snooping**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or firewall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the **ip dhcp snooping vlan** command (page 23-20), DHCP messages received on an untrusted interface (as specified by the **no ip dhcp snooping trust** command, page 23-24) from a device not listed in the DHCP snooping table will be dropped.
- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.
- Filtering rules are implemented as follows:
  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are

Downloaded from www.Manualslib.com manuals search engine

forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
  * If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
  * If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
  * If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the **ip dhcp snooping verify mac-address** command, page 23-21). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
  * If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (**ip dhcp snooping trust**, page 23-24). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages

Downloaded from www.Manualslib.com manuals search engine

from a DHCP server, any packets received from untrusted ports are dropped.

Example

This example enables DHCP snooping globally for the switch.

```
Console(config)#ip dhcp snooping
Console(config)#
```

Related Commands

ip dhcp snooping vlan (23-20)
ip dhcp snooping trust (23-24)

ip dhcp snooping vlan

This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

Syntax

[**no**] **ip dhcp snooping vlan** *vlan-id*

vlan-id - ID of a configured VLAN (Range: 1-4093)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- When DHCP snooping enabled globally using the **ip dhcp snooping** command (page 23-18), and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the **ip dhcp snooping trust** command (page 23-24).
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

Downloaded from www.Manualslib.com manuals search engine

- When DHCP snooping is globally enabled, configuration changes for specific VLANs have the following effects:
  - If DHCP snooping is disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

Related Commands

ip dhcp snooping (23-18)
ip dhcp snooping trust (23-24)

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

Syntax

[**no**] **ip dhcp binding verify mac-address**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

Example

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

ip dhcp snooping (23-18)
ip dhcp snooping vlan (23-20)
ip dhcp snooping trust (23-24)

ip dhcp snooping database write

This command writes all dynamically learned snooping entries to flash memory.

Command Mode

Global Configuration

Command Usage

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Example

```
Console(config)#ip dhcp snooping database write
Console(config)#
```

ip dhcp snooping service-provider-mode

This command converts the address assigned to a host by a DHCP server to a static entry in the MAC address table, and registers the host as a valid entry in the DHCP snooping table. Use the **no** form of this command disable this feature.

Syntax

[**no**] **ip dhcp service-provider-mode**

Default Setting

Disabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- This command applies to all VDSL ports. When set, it will automatically convert an address assigned to an attached CPE by a DHCP server to a static entry in the MAC address table. The MAC address, IP address, lease time, VLAN identifier, and port identifier are stored in the DHCP snooping table as a valid entry.
- If the lease time assigned by the DHCP server expires, or the connection between the switch and CPE is broken for any reason, the entry will be reset to a dynamic state.

Example

This example enable service provider mode globally on the switch.

```
Console(config)#ip dhcp snooping service-provider-mode
Console(config)#
```

ip dhcp snooping client limit

This command limits the number of host devices which can be attached to a VDSL port. Use the **no** form to restore the default setting.

Syntax

ip dhcp snooping client limit *number*
no ip dhcp snooping client limit

number - Maximum number of attached hosts. (Range: 1-48)

Default Setting

5

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The switch will monitor messages sent from a DHCP server to the attached hosts. Once the number of addresses assigned by the DHCP server reaches the client limit for an interface, no additional entries will be stored in the DHCP snooping table, and any subsequent

Downloaded from www.Manualslib.com manuals search engine

acknowledgement packets sent by the DHCP server in response to host requests will be blocked by the switch.

Example

This example sets the client limit to its maximum value on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip dhcp snooping client limit 48
Console(config-if)#
```

ip dhcp snooping trust

This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

Syntax

[**no**] **ip dhcp snooping trust**

Default Setting

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
- When DHCP snooping enabled globally using the **ip dhcp snooping** command (page 23-18), and enabled on a VLAN with the **ip dhcp snooping vlan** command (page 23-18), DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.

Downloaded from www.Manualslib.com manuals search engine

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

Example

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

Related Commands

ip dhcp snooping (23-18)
ip dhcp snooping vlan (23-20)

show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp snooping
Global DHCP Snooping status: enable
DHCP Snooping is configured on the following VLANs:
   1,
Verify Source Mac-Address: enable
Service Provider Mode: disable
Interface           Trusted        Client-limit
----------          ----------     ------------
Eth 1/1             No             5
Eth 1/2             No             5
Eth 1/3             No             5
Eth 1/4             No             5
Eth 1/5             Yes            5
⋮
```


Downloaded from www.Manualslib.com manuals search engine

show ip dhcp snooping binding

This command shows the DHCP snooping binding table entries.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec) Type                VLAN Interface
----------------- --------------- ---------- -------------------- ---- --------
11-22-33-44-55-66 192.168.0.99             0 Static-DHCPSNP          1 Eth 1/5
Console#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 24
ACCESS CONTROL LIST COMMANDS

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 24-1 Access Control List Commands

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/ UDP port number, protocol type, and TCP control code	24-2
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	24-16
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	24-26

Downloaded from www.Manualslib.com manuals search engine

IP ACLs

The commands in this section configure ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IP ACLs, first create an access list containing the required permit or deny rules, set a precedence mask to control the filter sequence, and then bind the access list to one or more ports

Table 24-2 IP ACL Commands

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IP ACLs	GC	24-3
permit, deny	Filters packets matching a specified source IP address	IP-STD-ACL	24-4
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	IP-EXT-ACL	24-5
show ip access-list	Displays the rules for configured IP ACLs	PE	24-7
access-list ip mask-precedence	Changes to the IP Mask mode used to configure access control masks	GC	24-8
mask	Sets a precedence mask for the ACL rules	IP-Mask	24-9
show access-list ip mask-precedence	Shows the ingress or egress rule masks for IP ACLs	PE	24-14
ip access-group	Adds a port to an IP ACL	IC	24-14
show ip access-group	Shows port assignments for IP ACLs	PE	24-14

Downloaded from www.Manualslib.com manuals search engine

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ip** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny 24-4
ip access-group (24-14)
show ip access-list (24-7)

Downloaded from www.Manualslib.com manuals search engine

permit, deny (Standard IP ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} {**any** | *source bitmask* | **host** *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard IP ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (24-3)

Downloaded from www.Manualslib.com manuals search engine

permit, deny (Extended IP ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]

[**no**] {**permit | deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- *precedence* – IP precedence level. (Range: 0-7)
- *tos* – Type of Service level. (Range: 0-15)
- *dscp* – DSCP priority level. (Range: 0-63)
- *sport* – Protocol[32] source port number. (Range: 0-65535)
- *dport* – Protocol[32] destination port number. (Range: 0-65535)
- *port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)

32. Includes TCP, UDP or other protocol types.

Downloaded from www.Manualslib.com manuals search engine

- *control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *flag-bitmask* – Decimal number representing the code bits to match.

Default Setting

None

Command Mode

Extended IP ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use "control-code 2 2"
  - Both SYN and ACK valid, use "control-code 18 18"
  - SYN valid and ACK invalid, use "control-code 2 18"

Downloaded from www.Manualslib.com manuals search engine

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
  destination-port 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-ext-acl)#
```

Related Commands

access-list ip (24-3)

show ip access-list

This command displays the rules for configured IP ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands

permit, deny 24-4
ip access-group (24-14)

access-list ip mask-precedence

This command changes to the IP Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified IP ACLs.

Command Mode

Global Configuration

Command Usage

- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#
```

Related Commands

mask (IP ACL) (24-9)
ip access-group (24-14)

mask (IP ACL)

This command defines a mask for IP ACLs. This mask defines the fields to check in the IP header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**protocol**]
{**any** | **host** | *source-bitmask*}
{**any** | **host** | *destination-bitmask*}
[**precedence**] [**tos**] [**dscp**]
[**source-port** [*port-bitmask*]] [**destination-port** [*port-bitmask*]]
[**control-flag** [*flag-bitmask*]]

- **protocol** – Check the protocol field.
- **any** – Any address will be matched.
- **host** – The address must be for a host device, not a subnetwork.
- *source-bitmask* – Source address of rule must match this bitmask.
- *destination-bitmask* – Destination address of rule must match this bitmask.
- **precedence** – Check the IP precedence field.
- **tos** – Check the TOS field.
- **dscp** – Check the DSCP field.
- **source-port** – Check the protocol source port field.
- **destination-port** – Check the protocol destination port field.
- *port-bitmask* – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **control-flag** – Check the field for control flags.
- *flag-bitmask* – Control flags of rule must match this bitmask. (Range: 0-63)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

IP Mask

Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and ingress or egress masks before mapping an ACL to an interface.
- If you enter **dscp**, you cannot enter **tos** or **precedence**. You can enter both **tos** and **precedence** without **dscp**.
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Example

This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```


Downloaded from www.Manualslib.com manuals search engine

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the "deny 10.1.1.1 255.255.255.255" rule has the higher precedence according the "mask host any" entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit any
Console(config-std-acl)#deny host 171.69.198.102
Console(config-std-acl)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A2 in
Console(config-if)#end
Console#show access-list
IP standard access-list A2:
  deny host 171.69.198.102
  permit any
Console#
```


Downloaded from www.Manualslib.com manuals search engine

This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23.

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any
  source-port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
  deny host 171.69.198.5 any
  deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
  deny 171.69.198.0 255.255.255.0 any source-port 23
  deny host 171.69.198.5 any
IP egress mask ACL:
  mask 255.255.255.0 any source-port
Console#
```


Downloaded from www.Manualslib.com manuals search engine

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL. Note that once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

```
Console(config)#access-list ip extended 6
Console(config-ext-acl)#permit any any
Console(config-ext-acl)#deny tcp any any control-flag 2 2
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask protocol any any control-flag 2
Console(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show access-list ip mask-precedence

This command shows the ingress or egress rule masks for IP ACLs.

Syntax

show access-list ip mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

```
Console#show access-list ip mask-precedence
IP ingress mask ACL:
  mask host any
  mask 255.255.255.0 any
Console#
```

Related Commands

mask (IP ACL) (24-9)

ip access-group

This command binds a port to an IP ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ip access-group** *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (24-7)

show ip access-group

This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
 IP standard access-list david
Console#
```

Related Commands

ip access-group (24-14)

Downloaded from www.Manualslib.com manuals search engine

MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, set a precedence mask to control the filter sequence, and then bind the access list to one or more ports

Table 24-3 MAC ACL Commands

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	24-17
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL	24-18
show mac access-list	Displays the rules for configured MAC ACLs	PE	24-20
access-list mac mask-precedence	Changes to the mode for configuring access control masks	GC	24-20
mask	Sets a precedence mask for the ACL rules	MAC-Mask	24-21
show access-list mac mask-precedence	Shows the ingress or egress rule masks for MAC ACLs	PE	24-24
mac access-group	Adds a port to a MAC ACL	IC	24-25
show mac access-group	Shows port assignments for MAC ACLs	PE	24-26

Downloaded from www.Manualslib.com manuals search engine

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list mac** *acl_name*

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny (24-18)
mac access-group (24-25)
show mac access-list (24-20)

Downloaded from www.Manualslib.com manuals search engine

permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

Note:- The default is for Ethernet II packets.

[**no**] {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

- **tagged-eth2** – Tagged Ethernet II packets.
- **untagged-eth2** – Untagged Ethernet II packets.
- **tagged-802.3** – Tagged Ethernet 802.3 packets.
- **untagged-802.3** – Untagged Ethernet 802.3 packets.
- **any** – Any MAC source or destination address.
- **host** – A specific MAC address.

Downloaded from www.Manualslib.com manuals search engine

- *source* – Source MAC address.
- *destination* – Destination MAC address range with bitmask.
- *address-bitmask*[33] – Bitmask for MAC address (in hexidecimal format).
- vid – VLAN ID. (Range: 1-4093)
- *vid-bitmask*[33] – VLAN bitmask. (Range: 1-4093)
- *protocol* – A specific Ethernet protocol number. (Range: 600-fff hex.)
- *protocol-bitmask*[33] – Protocol bitmask. (Range: 600-fff hex.)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype
 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (24-17)

33. For all bitmasks, "1" means care and "0" means ignore.

Downloaded from www.Manualslib.com manuals search engine

show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl_name*]

acl_name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny 24-18
mac access-group (24-25)

access-list mac mask-precedence

This command changes to MAC Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

Syntax

[**no**] **access-list ip mask-precedence** {**in** | **out**}

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

Default Setting

Default system mask: Filter inbound packets according to specified MAC ACLs.

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.

Example

```
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#
```

Related Commands

mask (MAC ACL) (24-21)
mac access-group (24-25)

mask (MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header. Use the **no** form to remove a mask.

Syntax

[**no**] **mask** [**pktformat**]
{**any** | **host** | *source-bitmask*} {**any** | **host** | *destination-bitmask*}
[**vid** [*vid-bitmask*]] [**ethertype** [*ethertype-bitmask*]]

- **pktformat** – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- **any** – Any address will be matched.
- **host** – The address must be for a single node.
- *source-bitmask* – Source address of rule must match this bitmask.
- *destination-bitmask* – Destination address of rule must match this bitmask.
- **vid** – Check the VLAN ID field.
- *vid-bitmask* – VLAN ID of rule must match this bitmask.

Downloaded from www.Manualslib.com manuals search engine

- **ethertype** – Check the Ethernet type field.
- *ethertype-bitmask* – Ethernet type of rule must match this bitmask.

Default Setting

None

Command Mode

MAC Mask

Command Usage

- Up to seven masks can be assigned to an ingress or egress ACL.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
  ff-ff-ff-ff-ff-ff any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
   permit any any
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any
  vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
   deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
   permit any any
MAC ingress mask ACL:
   mask pktformat host any vid
Console#
```


Downloaded from www.Manualslib.com manuals search engine

This example creates an Egress MAC ACL.

```
Console(config)#access-list mac M5
Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
 ff-ff-ff-ff-ff-ff any vid 3 ethertype 0806
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M5:
  deny tagged-802.3 host 00-11-11-11-11-11 any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
Console(config)#access-list mac mask-precedence out
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any
 vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#mac access-group M5 out
Console(config-if)#end
Console#show access-list
MAC access-list M5:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
  deny tagged-802.3 host 00-11-11-11-11-11 any
MAC ingress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

show access-list mac mask-precedence

This command shows the ingress or egress rule masks for MAC ACLs.

Syntax

show access-list mac mask-precedence [**in** | **out**]

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

Command Mode

Privileged Exec

Example

```
Console#show access-list mac mask-precedence
MAC egress mask ACL:
  mask pktformat host any vid ethertype
Console#
```

Related Commands

mask (MAC ACL) (24-21)

Downloaded from www.Manualslib.com manuals search engine

mac access-group

This command binds a port to a MAC ACL. Use the **no** form to remove the port.

Syntax

mac access-group *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (24-20)

Downloaded from www.Manualslib.com manuals search engine

show mac access-group

This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

Related Commands

mac access-group (24-25)

ACL Information

This section describes commands used to display ACL information.

Table 24-4 ACL Information Commands

Command	Function	Mode	Page
show access-list	Show all IP ACLs and associated rules	PE	24-26
show access-group	Shows the IP ACLs assigned to each port	PE	24-27

show access-list

This command shows all IP ACLs and associated rules.

Command Mode

Privileged Exec

Command Usage

Once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-group

This command shows the port assignments of IP ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
 IP standard access-list david
 MAC access-list jerry
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 25
INTERFACE COMMANDS

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Table 25-1 Interface Commands

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	25-2
description	Adds a description to an interface configuration	IC	25-3
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	25-3
negotiation	Enables autonegotiation of a given interface	IC	25-5
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	25-6
flowcontrol	Enables flow control on a given interface	IC	25-7
media-type	Force port type selected for combination ports	IC	25-8
switchport mdix	Sets pinout configuration to automatic detection or fixed mode	IC	25-9
shutdown	Disables an interface	IC	25-10
switchport packet-rate	Configures broadcast and multicast and unknown unicast storm control thresholds	IC	25-11
clear counters	Clears statistics on an interface	PE	25-12
show interfaces status	Displays status for the specified interface	NE, PE	25-13

Downloaded from www.Manualslib.com manuals search engine

Table 25-1 Interface Commands (Continued)

Command	Function	Mode	Page
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	25-14
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	25-16

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)
  - **port-channel** *channel-id* (Range: 1-12)
  - **vlan** *vlan-id* (Range: 1-4093)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

description

This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 1 Gbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Downloaded from www.Manualslib.com manuals search engine

Default Setting

- Auto-negotiation is permanently disabled on Ports 1-16, and enabled by default on Ports 17-19.
- When auto-negotiation is disabled, the default speed-duplex setting is:
  - Fast Ethernet ports – **100full** (100 Mbps full-duplex)
  - Gigabit Ethernet ports – **1000full** (1 Gbps full-duplex)

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (25-5)
capabilities (25-6)

Downloaded from www.Manualslib.com manuals search engine

negotiation

This command enables autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

[**no**] **negotiation**

Default Setting

Ports 1-16: Permanently disabled
Ports 17-19: Enabled

Command Mode

Interface Configuration (Ethernet - Ports 17-19, Port Channel)

Command Usage

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- When auto-negotiation is enabled the switch negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (25-6)
speed-duplex (25-3)

Downloaded from www.Manualslib.com manuals search engine

capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[**no**] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **1000full** - Supports 1 Gbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

100BASE-TX: 10half, 10full, 100half, 100full
1000BASE-T: 10half, 10full, 100half, 100full, 1000full
1000BASE-SX/LX/ZX (SFP): 1000full

Command Mode

Interface Configuration (Ethernet - Ports 17-19, Port Channel)

Command Usage

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must

Downloaded from www.Manualslib.com manuals search engine

manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#
```

Related Commands

negotiation (25-5)
speed-duplex (25-3)
flowcontrol (25-7)

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

Syntax

[**no**] **flowcontrol**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet - Ports 17-19, Port Channel)

Command Usage

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.

Downloaded from www.Manualslib.com manuals search engine

- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (25-5)
capabilities (flowcontrol, symmetric) (25-6)

media-type

This command forces the port type selected for combination ports 17-18. Use the **no** form to restore the default mode.

Syntax

media-type *mode*
no media-type

mode

Downloaded from www.Manualslib.com manuals search engine

- **copper-forced** - Always uses the built-in RJ-45 port.
- **sfp-forced** - Always uses the SFP port (even if module not installed).
- **sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

Default Setting

sfp-preferred-auto

Command Mode

Interface Configuration (Ethernet - Ports 17-18)

Example

This forces the switch to use the built-in RJ-45 port for the combination port 18.

```
Console(config)#interface ethernet 1/18
Console(config-if)#media-type copper-forced
Console(config-if)#
```

switchport mdix

This command sets pinout configuration to automatic detection or fixed mode for MDI/MDI-X signaling on the Gigabit Ethernet uplink ports. Use the **no** form to restore the default mode.

Syntax

switchport mdix {**auto** | **normal** | **crossover**}
no switchport mdix

- **auto** – Automatically detects the pinout configuration of the attached device, and negotiates with the link partner to determine which side will adjust the pinout signals if required to ensure a proper connection.
- **normal** – Specifies a fixed setting for MDI (i.e., straight-through).
- **crossover** – Specifies a fixed setting for MDI-X (i.e., crossover).

Default Setting

auto

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (Ethernet - Port 17-18)

Command Usage

Auto-negotiation must be enabled to use the "auto" option for this command. It must be disabled to force the pinout setting to one of the fixed modes of "normal" (MDI) or "crossover" (MDI-X).

One side of a link must be configured with MDI pinouts and the other side with MDI-X pinouts to ensure that signals sent from the transmit pins on one side of the link are received on the receive pins by the link partner. For more information on the signals used for each of these pinout types, refer to the Installation Guide.

Example

This forces the Port 18 to MDI mode.

```
Console(config)#interface ethernet 1/18
Console(config-if)#switchport mdix normal
Console(config-if)#
```

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[**no**] **shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport packet-rate

This command configures broadcast and multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

Syntax

switchport {**broadcast** | **multicast** | **unknown-unicast**}
packet-rate *rate*
no switchport {**broadcast** | **multicast** | **unknown-unicast**}

- **broadcast** - Specifies storm control for broadcast traffic.
- **multicast** - Specifies storm control for multicast traffic.
- **unknown-unicast** - Specifies storm control for unknown unicast traffic.
- *rate* - Threshold level as a rate; i.e., packets per second. (Range: 500-262143)

Default Setting

- Broadcast Storm Control: Enabled, packet-rate limit: 500 pps
- Multicast Storm Control: Enabled, packet-rate limit: 500 pps
- Unknown Unicast Storm Control: Enabled, packet-rate limit: 500 pps

Command Mode

Interface Configuration (Ethernet)

Command Usage

When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show interfaces status

This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status" on page 9-1.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A5
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full,
1000full
  Broadcast storm:        Enabled
  Broadcast storm limit:  500 packets/second
  Flow control:           Disabled
  LACP:                   Disabled
  Port security:          Disabled
  Max MAC count:          0
  Port security action:   None
  Media type:             None
Current status:
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 1000full
  Flow control type:      None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address:             00-00-AB-CD-00-00
Console#
```

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

Shows the counters for all interfaces.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port Statistics" on page 9-29.

Example

```
Console#show interfaces counters ethernet 1/17
Ethernet 1/17
 Iftable Stats:
  Octets Input: 30658, Octets Output: 196550
  Unicast Input: 6, Unicast Output: 5
  Discard Input: 0, Discard Output: 0
  Error Input: 0, Error Output: 0
  Unknown Protos Input: 0, QLen Output: 0
 Extended iftable Stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like Stats:
  Alignment Errors: 0, FCS Errors: 0
  Single Collision Frames: 0, Multiple Collision Frames: 0
  SQE Test Errors: 0, Deferred Transmissions: 0
  Late Collisions: 0, Excessive Collisions: 0
  Internal Mac Transmit Errors: 0, Internal Mac Receive Errors: 0
  Frames Too Long: 0, Carrier Sense Errors: 0
  In Pause Frames: 0, Out Pause Frames: 0
  Symbol Errors: 0
 RMON stats:
  Drop Events: 0, Octets: 227208, Packets: 3338
  Broadcast Pkts: 263, Multi-cast Pkts: 3064
  Undersize Pkts: 0, Oversize Pkts: 0
  Fragments: 0, Jabbers: 0
  CRC Align Errors: 0, Collisions: 0
  Packet Size <= 64 octets: 3150, Packet Size 65 to 127 octets: 139
  Packet Size 128 to 255 octets: 49, Packet Size 256 to 511 octets: 0
  Packet Size 512 to 1023 octets: 0, Packet Size 1024 to 1518 octets: 0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 4.

```
Console#show interfaces switchport ethernet 1/4
 Broadcast threshold:           Enabled, 500 packets/second
 LACP status:                   Disabled
 Ingress rate limit:            Disable, 1000M bits per second
 Egress rate limit:             Disable, 1000M bits per second
 VLAN membership mode:          Hybrid
 Ingress rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 GVRP status:                   Disabled
 Allowed VLAN:                     1(u),
 Forbidden VLAN:
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Table 25-2 show interfaces switchport - display description

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 25-11).
LACP status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 26-4).
Ingress/Egress rate limit	Shows if rate limiting is enabled, and the current rate limit (page 28-2).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 32-10).
Ingress rule	Shows if ingress filtering is enabled or disabled (page 32-12).
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 32-11).
Native VLAN	Indicates the default Port VLAN ID (page 32-13).
Priority for untagged traffic	Indicates the default priority for untagged frames (page 33-17).
GVRP status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 32-4).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 32-14).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 32-15).

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 26
LINK AGGREGATION COMMANDS

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 12 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 26-1 Link Aggregation Commands

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	25-2
channel-group	Adds a port to a trunk	IC (Ethernet)	26-3
Dynamic Configuration Commands			
lacp	Configures LACP for the current interface	IC (Ethernet)	26-4
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)	26-6
lacp admin-key	Configures a port's administration key	IC (Ethernet)	26-7

Downloaded from www.Manualslib.com manuals search engine

Table 26-1 Link Aggregation Commands (Continued)

Command	Function	Mode	Page
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)	26-8
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)	26-9
Trunk Status Display Commands			
show interfaces status port-channel	Shows trunk information	NE, PE	25-13
show lacp	Shows LACP information	PE	26-10

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).

Downloaded from www.Manualslib.com manuals search engine

- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-12)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[**no**] **lacp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A4
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0

 Current status:
  Created by:             Lacp
  Link status:            Up
  Operation speed-duplex: 1000full
  Flow control type:      None
  Member Ports:           Eth1/10, Eth1/11, Eth1/12,
Console#
```


Downloaded from www.Manualslib.com manuals search engine

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **system-priority** *priority*
no lacp {**actor** | **partner**} **system-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **admin-key** *key*
[**no**] **lacp** {**actor** | **partner**} **admin-key**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*
[**no**] **lacp admin-key**

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **port-priority** *priority*
no lacp {**actor** | **partner**} **port-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```


Downloaded from www.Manualslib.com manuals search engine

show lacp

This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

- *port-channel* - Local identifier for a link aggregation group. (Range: 1-12)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- **neighbors** - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Port channel: 1
---------------------------------------------------------------------
Eth 1/ 2
---------------------------------------------------------------------
  LACPDUs Sent:         10
  LACPDUs Receive:      5
  Marker Sent:          0
  Marker Receive:       0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
:
```


Downloaded from www.Manualslib.com manuals search engine

Table 26-2 show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Port channel: 1
------------------------------------------------------------------------
Oper Key:  3
Admin Key: 0
Eth 1/ 2
------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 32768
  LACP Port Priority:   32768
  Admin Key:            3
  Oper Key:             3
  Admin State:          defaulted, distributing, collecting,
                        synchronization, long timeout,
  Oper State:            distributing, collecting, synchronization,
                         aggregation, long timeout, LACP-activity
:
```

Table 26-3 show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.

Downloaded from www.Manualslib.com manuals search engine

Table 26-3 show lacp internal - display description (Continued)

Field	Description
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Downloaded from www.Manualslib.com manuals search engine

```
Console#show lacp 1 neighbors
Port channel 1 neighbors
-------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    32768, 00-01-F4-78-AE-C0
  Partner Admin Port Number: 2
  Partner Oper Port Number:  2
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                distributing, collecting, synchronization,
                             aggregation, long timeout, LACP-activity
.
.
.
```

Table 26-4 show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

Downloaded from www.Manualslib.com manuals search engine

```
Console#show lacp sysid
Port Channel     System Priority    System MAC Address
-----------------------------------------------------------------
           1               32768     00-30-F1-8F-2C-A7
           2               32768     00-30-F1-8F-2C-A7
           3               32768     00-30-F1-8F-2C-A7
           4               32768     00-30-F1-8F-2C-A7
           5               32768     00-30-F1-8F-2C-A7
           6               32768     00-30-F1-8F-2C-A7
           7               32768     00-30-F1-D4-73-A0
           8               32768     00-30-F1-D4-73-A0
           9               32768     00-30-F1-D4-73-A0
          10               32768     00-30-F1-D4-73-A0
          11               32768     00-30-F1-D4-73-A0
          12               32768     00-30-F1-D4-73-A0
:
```

Table 26-5 show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 27
MIRROR PORT COMMANDS

This section describes how to mirror traffic from a source port to a target port.

Table 27-1 Mirror Port Commands

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	27-1
show port monitor	Shows the configuration for a mirror port	PE	27-2

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *unit*/*port* (source port)
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-18)
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-18)

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 28
RATE LIMIT COMMANDS

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks, or for a VLAN member port. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Table 28-1 Rate Limit Commands

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	28-2
rate-limit snmp-trap-input	Sets an SNMP trap if traffic exceeds the configured rate limit	IC	28-3
show rate-limit vlan	Displays the rate limit for VLAN member ports	PE	28-4

Downloaded from www.Manualslib.com manuals search engine

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input** | **output** | **vlan** *vlan-id*} [*rate*]
no rate-limit {**input** | **output** | **vlan** [*vlan-id*]}

- **input** – Input rate for specified interface
- **output** – Output rate for specified interface
- **vlan** – Input rate for member port of specified VLAN
  - *vlan-id* - VLAN ID (Range: 1-4094)
- *rate* – Maximum value in Kbps (Range: 64 to 1024000 Kbps)

Default Setting

1024000 Kbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The rate limit may be set for both ingress and egress of any port or trunk. However, only the rate limit for ingress traffic can be controlled for a VLAN member port.
- Use the **no input vlan** command without a VLAN identifier to restore the default rate limit for the specified port on all VLANs for which it is a member. Use the **no input vlan** *vlan-id* command to restore the default rate limit for the specified VLAN.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#rate-limit vlan 1 640
Console(config-if)#
```

Related Command

show interfaces switchport (25-16)

Downloaded from www.Manualslib.com manuals search engine

rate-limit trap-input

This command sets an SNMP trap if traffic exceeds the configured rate limit. Use the **no** form to restore the default setting.

Syntax

rate-limit snmp-trap-input [**up** *upper-discard-boundary* **down** *lower-discard-boundary*]
no snmp-rate-limit trap-input

- *upper-discard-boundary* – The packet discard rate (per 10 second interval) above which the system sends a trap-input notification. (Range: 0-100000)
- *lower-discard-boundary* – The packet discard rate (per 10 second interval) below which the system sends another trap-input notification. (Range: 0-100000)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If the upper discard boundary is set to 0, then once the configured rate limit is exceeded (as specified by the **rate-limit** command, page 28-2), the system issues a trap message regardless of the discard rate.
- Once the system starts discarding packets in excess of a rate set for input, output, or a VLAN member port, and the upper discard boundary is exceeded, the system issues a trap-input notification. If the discard rate then falls beneath the lower discard boundary, the system will issue another trap-input notification.
- To prevent multiple trap-input messages from being sent when the discard rate fluctuates just above and below a boundary, the opposite boundary must first be crossed before another trap-input notification will be sent. However, note that this method is not applicable if the upper discard boundary is set to 0.

Downloaded from www.Manualslib.com manuals search engine

- For further information on the type of notification messages that can be sent by the system, refer to the information about trap and inform messages described under the **snmp-server host** command on page 21-6.

Example

This example sets an upper discard boundary of 500 packets / 10 seconds, and a lower discard boundary of 10 packets / 10 seconds.

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit snmp-trap-input up 500 down 10
Console(config-if)#
```

show rate-limit vlan

This command displays the rate limit for VLAN member ports.

Syntax

show rate-limit vlan [*vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Command Mode

Privileged Exec

Command Usage

Use this command without a VLAN identifier to display the configured rate limits for the port members of all VLANs, or enter a VLAN identifier to display the configured rate limit for all port members of the specified VLAN.

Example

```
Console#show rate-limit vlan
PORT   VLAN ID        Speed(Mbps)
1      1                    50
Console#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 29
VDSL COMMANDS

VDSL communication parameters can be set for individual ports, or multiple parameters can be defined in a profile and applied globally to the switch or to a group of ports. Alarm thresholds can be defined in a profile and then applied globally to the switch or to selected ports. The switch also provides an extensive listing of VDSL statistics.

For intelligent CPEs, firmware can be remotely upgraded.

Table 29-1 VDSL Commands

Command Groups	Function	Page
Long-Reach Ethernet*	Configures communication parameters for VDSL ports	29-2
Line Profile	Configures a list of communication parameters which can be applied to all VDSL ports or to a selected group of ports	29-35
Alarm Profile	Configures a list of threshold values for error states which can be applied all VDSL ports or to a selected group of ports	29-51
Displaying VDSL Information	Displays information on VDSL configuration settings, signal status, and communication statistics	29-61
CPE Configuration	Provides operation and maintenance (OAM) functions for remote customer premises equipment (CPE)	29-86

* Long-Reach Ethernet (LRE) is a technology that provides Ethernet-like performance over long-range connections using existing Category 1/2/3 voice-grade cabling. LRE can deliver voice, video and data services simultaneously without the need to rewire older buildings.

Downloaded from www.Manualslib.com manuals search engine

Long-Reach Ethernet Commands

This section describes how to configure communication parameters for VDSL ports such as specifying data band usage plans, setting notches within the frequency bands to avoid interference with ham radio signals, setting a mask for power spectral density to meet regional or local limitations for transmitting signals on phone lines, setting an acceptable target for the signal-to-noise ratio, and enabling automatic rate adaptation.

Table 29-2 Long-Reach Ethernet Commands

Command	Function	Mode	Page
lre band-plan	Sets the frequency bands used for VDSL signals	IC	29-4
lre option-band	Sets the frequencies to be used for the optional US0 band.	GC/IC	29-6
lre ham-band	Sets the HAM radio band that will be blocked to VDSL signals based on defined frequencies	GC/IC	29-7
lre region-ham-band	Sets the HAM radio band that will be blocked to VDSL signals based on defined usage types	GC/IC	29-9
lre psd-breakpoints	Sets the number of frequency breakpoints in the PSD mask	GC/IC	29-12
lre psd-frequencies	Maps a frequency to each breakpoint in the PSD mask	GC/IC	29-13
lre psd-value	Defines a power level for each of the PSD breakpoints	GC/IC	29-15
lre psd-mask-level	Sets a predefined PSD mask	GC/IC	29-16
lre pbo-config	Sets a mask to reduce the power spectral density (PSD) of transmitted signals at specified frequency breakpoints	GC	29-18
lre upbo	Enables upstream power backoff	GC/IC	29-19
lre tone	Disables VDSL signals at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz	GC/IC	29-21

Downloaded from www.Manualslib.com manuals search engine

Table 29-2 Long-Reach Ethernet Commands (Continued)

Command	Function	Mode	Page
lre max-power	Sets the maximum aggregate downstream or upstream power	GC/IC	29-22
lre min-protection	Configures the minimum level of impulse noise protection for all bearer channels	IC	29-23
lre channel	Sets the channel mode to fast or interleaved	IC	29-24
lre interleave-max-delay	Sets the maximum interleave delay	IC	29-25
lre datarate	Specifies the minimum and maximum data rate for downstream and upstream fast or slow (interleaved) channels	IC	29-26
lre rate-set	Sets the maximum input and output data rates for VDSL ports	GC/IC	29-27
lre noise-mgn target	Configures the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization	IC	29-28
lre noise-mgn min	Configures the minimum acceptable signal-to-noise margin	IC	29-28
lre shutdown	Shuts down a VDSL port	IC	29-30
lre reset	Resets the VDSL controller chip for the specified port or connected CPE	IC	29-30
lre auto-retraining	Initiates automatic retraining to find the optimal transmission rate when the link to a port is re-established	GC	29-31
lre retraining	Initiates the rate adaptation method to find the optimal transmission rate based on existing line conditions	IC	29-32
lre rate-adaption	Enables line rate adaptation which can set the optimal transmission rate based on existing line conditions	GC/IC	29-33
lre apply	Applies all global VDSL settings to each port, overwriting any previous settings configured for specific interfaces	GC/IC	29-34

Downloaded from www.Manualslib.com manuals search engine

lre band-plan

This command sets the frequency bands used for VDSL signals based on a set of predefined plans. Use the **no** form to restore the default status.

Syntax

lre band-plan *value*
no lre band-plan

value – Index for a predefined band plan.
(See Table 29-3, "VDSL2 Band Plans," on page 29-5.)

Default Setting

5 (100/100)

Command Mode

Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to set a band plan for a designated usage type for all VDSL ports, or in interface mode to set a plan for a specific VDSL port.
- The band plan options provided by this command are described by ITU-T Standards G.9932. The first field in the band plan designator indicates the ITU standard, the second field indicates the lower frequency bound, and the third field indicates the upper frequency bound.
- This switch is specifically designed to support Band Plan 5 – G.993.2, Annex C for Japan. Careful testing should be carried out before using any other band plans. The following table lists the predefined band plans. Note that band plan designators starting with 997 are primarily for use in the European Union, those starting with 998 are mainly for use in North America.

Downloaded from www.Manualslib.com manuals search engine

Table 29-3 VDSL2 Band Plans

Index	Designator
3	998-138-8500 Long Reach
4	998-138-12000 High Data Rate
5	998-640-30000 100/100
6	997-138-8500
7	Flex-138-4400
8	998-138-4400
9	997-138-4400
11	998-138-4400-optBand
12	997-138-4400-optBand
18	998-138-12000 4K Tones
19	997-138-12000 4K Tones
20	998-138-17000 4K Tones

Example

This example sets the band plan to 998-640-30000.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre band-plan 5
Console(config-if)#
```

Related Commands

show lre (29-79)

Downloaded from www.Manualslib.com manuals search engine

lre option-band

This command sets the frequencies to be used for the optional Upstream Band 0 (US0). Use the **no** form to restore the default status.

Syntax

lre option-band *value*
no lre option-band

value – Index of predefined frequency bounds for US0. Note that each option includes a range for the low and high end frequencies. (Options:0 - No optional band
1 - ITU-T G993.2, Annex A, 6-32 kHz, 26-138 kHz
2 - ITU-T G993.2, Annex B, 32-64 kHz, 138-276 kHz
3 - ITU-T G993.2, Annex B, 6-64 kHz, 26-276 kHz)

Default Setting

0 (No optional band)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to configure the US0 band for all VDSL ports, or in interface mode to configure it for a specific VDSL port.
- Performance enhancements have been incorporated in G.993.2 for the optional US0 band (specifically, support in initialization for training of time domain equalizers and echo cancellers).

Example

This example sets configures the frequency bounds for US0 to 6-32 KHz.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre option-band 2
Console(config-if)#
```

Related Commands

show lre option-band (29-63)

Downloaded from www.Manualslib.com manuals search engine

lre ham-band

This command sets the Handheld Amateur Radio (HAM) band that will be blocked to VDSL signals based on defined frequencies. Use the **no** form to restore the default status.

Syntax

lre ham-band *value*
no lre ham-band

value – HAM band mask.
(See Table 29-4, "HAM Band Notches," on page 29-7.)

Default Setting

22 (none)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to set a HAM band mask for all VDSL ports, or in interface mode to set a mask for a specific VDSL port.
- Using a HAM band mask prevents interference with other systems (e.g., amateur radio) that use narrow band transmission in the VDSL frequency band. The selected frequency range will not be used to transmit data on the VDSL line. You may need to specify a mask if required by local regulations or if specific incidents of interference are reported within a service area.
- The following table lists the HAM band notches.

Table 29-4 HAM Band Notches

Index	Name	Frequency	Reference
1	RFI-BAND01	1.810 - 1.825 MHz	ANNEX F
2	RFI-BAND02	1.810 - 2.000 MHz	ETSI, T1E1
3	RFI-BAND03	1.9075 - 1.9125 MHz	ANNEX F

Downloaded from www.Manualslib.com manuals search engine

Table 29-4 HAM Band Notches (Continued)

Index	Name	Frequency	Reference
4	RFI-BAND04	3.500 - 3.575 MHz	ANNEX F
5	RFI-BAND05	3.500 - 3.800 MHz	ETSI
6	RFI-BAND06	3.500 - 4.000 MHz	T1E1
7	RFI-BAND07	3.747 - 3.754 MHz	ANNEX F
8	RFI-BAND08	3.791 - 3.805 MHz	ANNEX F
9	RFI-BAND09	7.000 - 7.100 MHz	ANNEX F, ETSI
10	RFI-BAND10	7.000 - 7.300 MHz	T1E1
11	RFI-BAND11	10.100 - 10.150 MHz	ANNEX F, ETSI, T1E1
12	RFI-BAND12	14.000 - 14.350 MHz	ANNEX F, ETSI, T1E1
13	RFI-BAND13	18.068 - 18.168 MHz	ANNEX F, ETSI, T1E1
14	RFI-BAND14	1.800 - 1.825 MHz	HAM Band 1
15	RFI-BAND15	3.500 - 3.550 MHz	HAM Band 2
16	RFI-BAND16	3.790 - 3.800 MHz	HAM Band 3
17	RFI-BAND17	1.800 - 1.810 MHz	RFI Notch
18	RFI-BAND18	21.000 - 21.450 MHz	ANNEX F, ETSI, T1E1
19	RFI-BAND19	24.890 - 24.990 MHz	ANNEX F, ETSI, T1E1
20	RFI-BAND20	28.000 - 29.100 MHz	ANNEX F, ETSI, T1E1
21	RFI-BAND21	28.000 - 29.700 MHz	ANNEX F, ETSI, T1E1
22	RESET-ALL-OFF	null frequency mask	

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets a HAM band notch in the transmitted power spectrum in the 10.000 - 10.150 MHz transmission band (also called the 30 meter band).

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre ham-band 11
Console(config-if)#
```

Related Commands

show lre ham-band (29-64)
lre region-ham-band (29-9)

lre region-ham-band

This command sets the ham radio band that will be blocked to VDSL signals based on defined usage types. Use the **no** form to restore the default status.

Syntax

lre region-ham-band *value*
no lre region-ham-band

value – HAM band mask for designated usage type.
(See Table 29-5, "HAM Band Notches for Usage Types," on page 29-10.)

Default Setting

36 (none)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to set a HAM band mask for a designated usage type for all VDSL ports, or in interface mode to set a mask for a specific VDSL port.

Downloaded from www.Manualslib.com manuals search engine

- Using a HAM band mask prevents interference with other systems (e.g., amateur radio) that use narrow band transmission in the VDSL frequency band. The selected frequency range will not be used to transmit data on the VDSL line. You may need to specify a mask if required by local regulations or if specific incidents of interference are reported within a service area.
- The following table lists HAM band notches for general usage types.

Table 29-5 HAM Band Notches for Usage Types

Index	Name	Frequency	Reference
1	RFI-BAND01	1.800 - 2.000 MHz	Amateur Radio
2	RFI-BAND02	2.173 - 2.191 MHz	GMDSS*
3	RFI-BAND03	2.850 - 3.155 MHz	Aeronautical Communications
4	RFI-BAND04	3.400 - 3.500 MHz	Aeronautical Communications
5	RFI-BAND05	3.500 - 3.800 MHz	Amateur Radio
6	RFI-BAND06	3.800 - 4.000 MHz	Aeronautical/Broadcasting
7	RFI-BAND07	4.200 - 4.215 MHz	GMDSS
8	RFI-BAND08	4.650 - 4.850 MHz	Aeronautical Communications
9	RFI-BAND09	5.450 - 5.730 MHz	Aeronautical Communications
10	RFI-BAND10	5.900 - 6.200 MHz	DRM Radio†
11	RFI-BAND11	6.300 - 6.320 MHz	GMDSS
12	RFI-BAND12	6.525 - 6.765 MHz	Aeronautical Communications
13	RFI-BAND13	7.000 - 7.200 MHz	Amateur Radio
14	RFI-BAND14	7.200 - 7.450 MHz	DRM Radio
15	RFI-BAND15	8.405 - 8.420 MHz	GMDSS
16	RFI-BAND16	8.815 - 9.040 MHz	Aeronautical Communications
17	RFI-BAND17	9.400 - 9.900 MHz	DRM Radio

Downloaded from www.Manualslib.com manuals search engine

Table 29-5 HAM Band Notches for Usage Types (Continued)

Index	Name	Frequency	Reference
18	RFI-BAND18	10.005 - 10.100 MHz	Aeronautical Communications
19	RFI-BAND19	10.100 - 10.150 MHz	Amateur Radio
20	RFI-BAND20	11.175 - 11.400 MHz	Aeronautical Communications
21	RFI-BAND21	11.600 - 12.100 MHz	DRM Radio
22	RFI-BAND22	12.570 - 12.585 MHz	GMDSS
23	RFI-BAND23	13.200 - 13.360 MHz	Aeronautical Communications
24	RFI-BAND24	13.570 - 13.870 MHz	DRM Radio
25	RFI-BAND25	14.000 - 14.350 MHz	Amateur Radio
26	RFI-BAND26	15.010 - 15.100 MHz	Aeronautical Communications
27	RFI-BAND27	15.100 - 15.800 MHz	DRM Radio
28	RFI-BAND28	16.795 - 16.810 MHz	GMDSS
29	RFI-BAND29	17.480 - 17.900 MHz	DRM Radio
30	RFI-BAND30	17.900 - 18.030 MHz	Aeronautical Communications
31	RFI-BAND31	18.068 - 18.168 MHz	Amateur Radio
32	RFI-BAND32	21.000 - 21.450 MHz	Amateur Radio
33	RFI-BAND33	24.890 - 24.990 MHz	Amateur Radio
34	RFI-BAND34	26.965 - 27.405 MHz	CB Radio‡
35	RFI-BAND35	28.000 - 29.700 MHz	Amateur Radio
36	RESET-ALL-OFF	null frequency mask	
37	NO-REGION	null frequency mask	

* Global Maritime Distress and Safety System
† Digital Radio Mondiale (Digital Radio Broadcasting)
‡ Citizen's Band Radio

Downloaded from www.Manualslib.com manuals search engine

Example

This example sets a HAM band notch in the transmitted power spectrum to avoid interference with CB radios.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre region-ham-band 34
Console(config-if)#
```

Related Commands

show lre region-ham-band (29-65)
lre ham-band (29-7)

lre psd-breakpoints

This command sets the number of frequency breakpoints in the PSD mask. Use the **no** form to restore the default setting.

Syntax

lre psd-breakpoints *number*
no lre psd-breakpoints

number – The number of frequency breakpoints used in the PSD mask. (Range: 0-28)

Default Setting

28

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to configure the number of breakpoints for all VDSL ports, or in interface mode to configure it for a specific VDSL port.
- Breakpoints are associated with a signal frequency using the lre psd-frequencies command (page 29-13), and used in conjunction with the power levels defined by the lre psd-value command (page 29-15) to create a PSD mask used for in-band spectrum shaping, set the Limit

Downloaded from www.Manualslib.com manuals search engine

PSD Mask required for compliance with local regulations, or set mask limits for upstream power backoff. The methods used to calculate these various PSD masks, and local regulations governing the power spectrum used on VDSL lines are all described in ITU-T G.993.2.

- Breakpoints can be applied to any upstream or downstream channel depending on the associated frequencies.

Example

The following sets 25 breakpoints on VDSL port 1. This allows five breakpoints to be set for each of DS1, US1, DS2, US2 and DS3 upstream and downstream channels. This would allow you to set a steep slope at the channel bounds, as well as a small peak toward the center of the band.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre psd-breakpoint 25
Console(config-if)#
```

Related Commands

lre psd-frequencies (29-13)
lre psd-value (29-15)
show lre psd (29-67)
lre psd-mask-level (29-16)

lre psd-frequencies

This command maps a frequency to each breakpoint in the PSD mask. Use the **no** form to restore the default setting.

Syntax

lre psd-frequencies *breakpoint frequency*

- *breakpoint* – One of the breakpoints defined by the **lre psd-breakpoints** command (page 29-12).
- *frequency* – A frequency assigned to the corresponding breakpoint. (Range: 0-30000 kHz)

Default Setting

none

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to configure frequency breakpoints for all VDSL ports, or in interface mode to configure them for a specific VDSL port.
- The number of breakpoints used in the PSD mask is specified with the **lre psd-breakpoints** command (page 29-12), while the power level set for each breakpoint is defined by the **lre psd-value** command (page 29-15). These PSD commands are used to create a PSD mask for in-bank spectrum shaping, setting the Limit PSD Mask required for compliance with local regulations, or setting mask limits for upstream power backoff. The methods used to calculate these various PSD masks, and local regulations governing the power spectrum used on VDSL lines are all described in ITU-T G.993.2.

Example

The following sets breakpoint frequencies for US1 to create a slope at the channel bounds, and peak at the center of the band.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre psd-frequencies 1 3750
Console(config-if)#lre psd-frequencies 2 3900
Console(config-if)#lre psd-frequencies 3 4475
Console(config-if)#lre psd-frequencies 4 5050
Console(config-if)#lre psd-frequencies 5 5200
Console(config-if)#
```

Related Commands

lre psd-breakpoints (29-12)
lre psd-value (29-15)
show lre psd (29-67)
lre psd-mask-level (29-16)

Downloaded from www.Manualslib.com manuals search engine

lre psd-value

This command defines a power level for each of the PSD breakpoints. Use the **no** form to restore the default setting.

Syntax

lre psd-value *breakpoint psd-value*
no lre psd-value *breakpoint*

- *breakpoint* – Frequency breakpoint within the power spectral density (PSD) as defined by the **lre psd-breakpoints** command (page 29-12).
- *psd-value* – Value of PSD at the specified breakpoint. (Range: An integer from 0 to 255, which is used to calculate a power level in terms of -140 + (*psd-value*) * 0.5 dBm/Hz)

Default Setting

255 (-12.5 dBm/Hz)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to configure a PSD value for all VDSL ports, or in interface mode to configure it for a specific VDSL port.
- The PSD values are used in conjunction with the frequency breakpoints (defined by the **lre psd-breakpoints** and **lre psd-frequencies** commands, page 29-12 and 29-13) to create a PSD mask used for in-band spectrum shaping, set the Limit PSD Mask required for compliance with local regulations, or set mask limits for upstream power backoff. The methods used to calculate these various PSD masks, and local regulations governing the power spectrum used on VDSL lines are all described in ITU-T G.993.2.
- Note that settings for the MIB PSD mask can only be configured through an SNMP network management interface.

Downloaded from www.Manualslib.com manuals search engine

Example

The following sets a PSD value for the frequency band bounded by breakpoints 1 and 2 to -20 dBm/Hz on VDSL port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre psd-value 1 240
Console(config-if)#lre psd-value 2 240
Console(config-if)#
```

Related Commands

lre psd-breakpoints (29-12)
lre psd-frequencies (29-13)
show lre psd (29-67)
lre psd-mask-level (29-16)

lre psd-mask-level

This command sets a predefined PSD mask. Use the **no** form to restore the default setting.

Syntax

lre psd-mask-level *value*
no lre psd-mask-level

value – Index for a predefined PSD mask.
(See Table 29-6, "PSD Mask Options," on page 29-17.)

Default Setting

5 (Annex F)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to set a predefined PSD mask for all VDSL ports, or in interface mode to set a mask for a specific VDSL port. Note that this switch is specifically designed to meet the requirements for G.993.2, Annex C for Japan. We do not therefore recommend changing the mask without careful testing.

Downloaded from www.Manualslib.com manuals search engine

- The following table lists the predefined band plans.

Table 29-6 PSD Mask Options

Index	Designator
0	Default PSD
1	ANSI M1_CAB
2	ANSI M2_CAB
3	ETSI M1_CAB
4	ETSI M2_CAB
5	ANNEX F
6	ANSI M1_EX
7	ANSI M2_EX
8	ETSI M1_EX
9	ETSI M2_EX
10	Reserved
11	PSD K
12	PSD_CHINA
13	ETSI_M1_EX_P1
14	ETSI_M2_EX_P1

Example

The following specifies a predefined mask based on Annex F of ITU-T G.993.1 for use on VDSL port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre psd-mask-level 5
Console(config-if)#
```

Related Commands

show lre psd-mask-level (29-68)
lre psd-breakpoints (29-12)
lre psd-frequencies (29-13)
lre psd-value (29-15)

Downloaded from www.Manualslib.com manuals search engine

lre pbo-config

This command sets a mask to reduce the power spectral density (PSD) of transmitted signals at specified frequency breakpoints for upstream power backoff. Use the **no** form to restore the default status.

Syntax

lre pbo-config
K1[0] *Rx_PSD1* **K1[1]** *Rx_PSD2* **K1[2]** *Rx_PSD3*
K1[3] *Rx_PSD4* **K1[4]** *Rx_PSD5* **K1[5]** *Rx_PSD6*
K2[0] *Tx_PSD1* **K2[1]** *Tx_PSD2* **K2[2]** *Tx_PSD3*
K2[3] *Tx_PSD4* **K2[4]** *Tx_PSD5* **K2[5]** *Tx_PSD6*
no lre pbo-config

- **K1[0-5]** – Frequency breakpoints for upstream bands DS1-DS3.
- *Rx_PSD1-6* – Limitation on the PSD at specified breakpoint. (Range: -1000000 to 1000000, in units of 1000 x decibel)
- **K2[0-5]** – Frequency breakpoints for downstream bands US0-US2.
- *Tx_PSD1-6* – Limitation on the PSD at specified breakpoint. (Range: -1000000 to 1000000, in units of 1000 x decibel)

Default Setting

K1[0] 0 K1[1] -60000 K1[2] -60000 K1[3] -60000 K1[4] 0 K1[5] 0
K2[0] 0 K2[1] -11200 K2[2] -7419 K2[3] -7419 K2[4] 0 K2[5] 0

Command Mode

Global Configuration

Command Usage

- The PSD values specified by this command are in units of 1000 x decibel (dB). For example, 60000 means 60.0 dB. The actual power levels implemented are in milliwatts per Hertz (dBm/Hz). For example, you would enter -60000 with this command to specify a value of -60 dBm/Hz.
- Upstream power back-off (UPBO) is used to mitigate far-end crosstalk caused by upstream transmissions from shorter to longer loops. The **lre pbo-config** command is used to reshape the PSD, ensuring that the signals on short to long loops are compatible.

Downloaded from www.Manualslib.com manuals search engine

- The transceiver will adjust its transmitted signal to conform to the power limitations set by the **lre pbo-config** command.
- If upstream power backoff is enabled with the **lre upbo** command (page 29-19), the transceiver will automatically reduce the PSD at each frequency breakpoint set the by the **lre psd-breakpoints** (page 29-12) and **lre psd-frequencies** (page 29-13) commands.

Example

This example sets PSD values for downstream bands at 0 -60 -60 -60 0 0 dBm/Hz, and for upstream bands at 0 -11.2 -7.419 -7.419 0 0 dBm/Hz.

```
Console(config)#
Console(config)#lre pbo-config k1[0] 0 k1[1] -60000 k1[2] -60000
  k1[3] -60000 k1[4] 0  k1[5] 0 k2[0] 0 k2[1] -11200 k2[2] -7419
  k2[3] -7419 k2[4] 0 k2[5] 0
Console(config)#
```

Related Commands

lre upbo (29-19)
show lre pbo-config (29-69)
lre psd-breakpoints (29-12)
lre psd-frequencies (29-13)

lre upbo

This command enables upstream power backoff. Use the **no** form to restore the default setting.

Syntax

[**no**] **lre upbo**

Default Setting

disabled

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Enter this command in global configuration mode to enable upstream power backoff for all VDSL ports, or in interface mode to enable it for a VDSL port.
- Upstream power backoff (UPBO) should be configured when there are VDSL connections of different lengths attached to this switch. UPBO is required to improve the spectral compatibility on lines of different lengths by reducing the transmitted power on shorter lines. If UPBO is enabled by this command, and a PBO mask has been defined, the transceiver will use the PBO mask.
- This command will apply the upstream power backoff PSD mask to the specified ports based on configuration settings specified with the **lre pbo-config** command (page 29-18) as described in ITU-T G.992.2. If UPBO is enabled, but a PBO mask has not been configured, the specified transceiver will automatically control upstream power backoff based on default values set by the DSP engine.

Example

This example enables upstream power backoff on port 1.

```
Console(config)interface ethernet 1/1#
Console(config-if)#lre upbo
Console(config-if)#
```

Related Commands

show lre upbo (29-70)
lre pbo-config (29-18)

Downloaded from www.Manualslib.com manuals search engine

lre tone

This command disables VDSL signals at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz. Use the **no** form to restore the default setting.

Syntax

lre tone {**tx** | **rx**} *value*
no lre tone {**tx** | **rx**}

- **tx** – Downstream band plan.
- **rx** – Upstream band plan.
- *value* – Index of low-end frequency range to disable.
  (Options:1 - all tones on
  2 - disable tones at 640 KHz and below
  3 - disable tones at 1.1 MHz and below
  4 - disable tones at 2.2 MHz and below)

Default Setting

3 (disable tones at 1.1 MHz and below)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to disable the specified low-end frequency for all VDSL ports, or in interface mode to disable it for a VDSL port.
- This command specifies a frequency beneath which VDSL signals are not allowed. For example, the default lower frequency bound for DS1 defined in Annex C of G.993.2 is 640 KHz. The low-end frequencies filtered out by this command are used for common POTS or ISDN services.
- The frequency bound specified by this command takes precedence over that defined in the selected band plan (see **lre band-plan**, page 29-4).

Downloaded from www.Manualslib.com manuals search engine

Example

The following disables all tone beneath 640 kHz on the upstream band plan.

```
Console(config)#
Console(config)#lre tone tx 2
Console(config)#
```

Related Commands

show lre tone (29-71)

lre max-power

This command sets the maximum aggregate downstream or upstream power. Use the **no** form to restore the default setting.

Syntax

lre max-power {**down** | **up**} *value*
no lre max-power {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Maximum aggregate power. (Range: 0-255, in units of 0.25 dBm)

Default Setting

255 (63.75 dBm)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

Enter this command in global configuration mode to set the maximum aggregate power for all VDSL ports, or in interface mode to set it for a specific VDSL port.

Downloaded from www.Manualslib.com manuals search engine

Example

The following sets the maximum downstream power on port 1 to 14.5 dBm.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre max-power down 58
Console(config-if)#
```

lre min-protection

This command configures the minimum level of impulse noise protection for all bearer channels. Use the **no** form to restore the default setting.

Syntax

lre min-protection {**down** | **up**} *value*
no lre max-power {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – The number of consecutive DMT symbols for which errors can be completely corrected. (Range: 0-255, in units of 0.5 DMT symbols, or 125 microseconds)

Default Setting

0

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- This minimum margin indicates the amount of increase in impulse noise that the system can tolerate under operational conditions while still ensuring required transmission quality.
- This command is used to set the time span of impulse noise protection, as seen at the input to the de-interleaver, for which errors can be completely corrected by the error correcting code, regardless of the number of errors within the errored DMT symbols.

Downloaded from www.Manualslib.com manuals search engine

- Note that this parameter only applies to interleaved channels. Refer to ITU-T G.993.2 for a full description of the methods used to calculate the minimum level of impulse noise protection.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lr min-protection down 5
Console(config-if)#
```

lre channel

This command sets the channel mode to fast or interleaved. Use the **no** form to restore the default status.

Syntax

lre channel *mode*
no lre channel

mode – Channel mode (Options: fast, interleave)

Default Setting

interleaved

Command Mode

Interface Configuration (VDSL Port)

Command Usage

- Interleaving protects data against bursts of errors by using the Reed-Solomon error correction algorithm to spread the errors over a number of code words. A greater degree of interleaving provides more protection against noise pulses, but increases transmission delay and reduces the effective bandwidth.
- For applications that cannot tolerate latency (for example, voice), use the fast mode to disable the interleaving burst error correction method.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre channel interleave
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre interleave-max-delay (29-25)

lre interleave-max-delay

This command sets the maximum interleave delay. Use the **no** form to restore the default status.

Syntax

lre interleave-max-delay {**down** | **up**} *value*
no lre interleave-max-delay {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Maximum interleave delay. (Range: 0-40, indicating units of 0.5 ms)

Default Setting

4 (2 ms)

Command Mode

Interface Configuration (VDSL Port)

Command Usage

- Interleaving causes a delay in the transmission of data.
- Setting the interleave delay to a value of zero disables interleaving.
- Interleave delay applies only to the interleave (slow) channel and defines the mapping (relative spacing) between subsequent input bytes at the interleaver input and their placement in the bit stream at the interleaver output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream allowing for improved impulse noise immunity at the expense of payload latency.

Example

This example sets the interleave delay to 3 milliseconds.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre interleave-max-delay down 6
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre channel (29-24)
show lre interleave-max-delay (29-72)

lre datarate

This command specifies the minimum and maximum data rate for downstream and upstream fast or slow (interleaved) channels. Use the **no** form to restore the default setting.

Syntax

lre datarate {**down** | **up**} {**slow** | **fast**} {**max** | **min**} *value*
no lre datarate {**down** | **up**} {**slow** | **fast**} {**max** | **min**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- **slow** – Slow (interleaved) channel.
- **fast** – Fast channel.
- **max** – Maximum channel data rate.
- **min** – Minimum channel data rate.
- *value* – The data rate. (Range: 1-200,000 kbps)

Default Setting

Maximum data rate: 200,000 kbps
Minimum data rate: 64 kbps

Command Mode

Interface Configuration (VDSL Port)

Command Usage

The command sets the minimum and maximum data rates supported by each upstream and downstream band. Bounding data rates should be set for both fast and slow channels if operation may sometimes disable or enable interleaving. These bounds are applied to the specified interface when rate adaption is enabled (see **Command Usage**, page 29-32).

Downloaded from www.Manualslib.com manuals search engine

Example

The following sets the minimum and maximum data rates for the downstream fast channel on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre datarate down fast max 190000
Console(config-if)#lre datarate down fast min 640
Console(config-if)#
```

Related Commands

show lre rate-adaption (29-75)
show lre datarate (29-73)
lre rate-set (29-27)

lre rate-set

This command sets the maximum input and output data rates for the VDSL ports. Use the **no** form to restore the default setting.

Syntax

lre rate-set {**input** | **output**} *value*
no lre rate-set {**input** | **output**}

- **input** – Downstream traffic from the service provider.
- **output** – Upstream traffic to the service provider.
- *value* – The data rate. (Range: 1-200,000 kbps)

Default Setting

Auto-retraining (see page 29-31)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Example

The following sets the maximum data rates for port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre rate-set input 200000
Console(config-if)#lre rate-set output 100000
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre datarate (29-26)

lre noise-mgn target

This command configures the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization. Use the **no** form to restore the default setting.

Syntax

lre noise-mgn target {**down** | **up**} *value*
no lre noise-mgn target {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Signal-to-noise margin. (Range: 0-62, in units of 0.5 dB)

Default Setting

12 dB

Command Mode

Interface Configuration (VDSL Port)

Command Usage

This command sets the noise margin that transceivers must achieve with a Bit Error Rate (BER) of 10^{-7} or better to successfully complete initialization. It indicates the maximum amount by which the reference crosstalk noise level can be increased during a BER test without causing the modem to fail the BER requirement.

Example

The following sets a targeted SNR of 15 dB on Port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre noise-mgn target down 30
Console(config-if)#
```

Related Commands

lre noise-mgn min (29-29)
show lre noise-mgn (29-74)

Downloaded from www.Manualslib.com manuals search engine

lre noise-mgn min

This command configures the minimum acceptable signal-to-noise margin. Use the **no** form to restore the default setting.

Syntax

lre noise-mgn min {**down** | **up**} *value*
no lre noise-mgn min {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Signal-to-noise margin. (Range: 0-62, in units of 0.5 dB)

Default Setting

10 dB

Command Mode

Interface Configuration (VDSL Port)

Command Usage

- This command sets the minimum noise margin the receiver can tolerate. If the noise margin falls below this level, the receiver will ask the sender to increase its transmit power. If it is not possible to increase the transmit power, a loss-of-margin defect occurs, the link will fail and the receiver will attempt to re-initialize.
- When rate adaptation is enabled (see Command Usage, page 29-32), the signal-to-noise ratio (SNR) is an indicator of link quality. The switch itself has no internal functions to ensure link quality. To ensure a stable link, you should add a margin to the theoretical minimum signal-to-noise ratio (SNR).

Example

The following sets the minimum noise margin on port 1 to 14 dB.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre noise-mgn min down 28
Console(config-if)#
```

Related Commands

lre noise-mgn target (29-28)

Downloaded from www.Manualslib.com manuals search engine

lre shutdown

This command shuts down a VDSL port. Use the **no** form to re-enabled a port.

Syntax

[**no**] **lre shutdown**

Default Setting

All VDSL ports are operational

Command Mode

Interface Configuration (VDSL Port)

Command Usage

Use this command to disable the VDSL chipset transmitter of a VDSL port that is not connected to a working CPE. In some unusual circumstances, the power emitted by VDSL ports can affect other VDSL ports. It is recommended that ports that are not wired to CPEs be shut down in this way. Also use this command to disable access to the switch from this port for troubleshooting or security reasons.

Example

The following example disables VDSL port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre shutdown
Console(config-if)#
```

lre reset

This command resets the VDSL controller chip for the specified VDSL port or the connected CPE. Use the **no** form to re-enabled a port.

Syntax

lre reset {**local** | **remote**}

- **local** – VDSL2 chip at specified switch port.
- **remote** – VDSL2 chip at CPE connected to specified switch port.

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (VDSL Port)

Command Usage

Use this command to troubleshoot VDSL connection or performance problems.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre reset remote
Console(config-if)#lre reset local
Console(config-if)#
```

lre auto-retraining

This command initiates automatic retraining to find the optimal transmission rate when the switch re-establishes the link to a port. Use the **no** form to disable this feature.

Syntax

[**no**] **lre auto-retraining**

Default

Enabled

Command Mode

Global Configuration

Command Usage

- When auto-retraining is enabled and the link to a port drops, that port will automatically enter retraining and connect at the optimum rate based on the bounds defined by the **lre datarate** command (page 29-26).
- If auto-retraining is not enabled, the link can only be brought up by manually by entering the **lre retraining** command (page 29-32) after the link to a port drops.

Example

```
Console(config)#lre auto-retraining
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre datarate (29-26)

lre retraining

This command manually initiates the rate adaptation method to find the optimal transmission rate based on existing line conditions. Use the **no** form to disable this feature.

Default

Disabled

Command Mode

Interface Configuration (VDSL Port)

Command Usage

- This command can be used if auto-retraining has been disabled with the **no lre auto-retraining** command (page 29-31), and the signal quality or link on a port has dropped. The **lre-retraining** command will initiate rate adaptation and select the optimal transmission rate based on existing line conditions and the bounds set by the **lre datarate** command (page 29-26).
- Note that it might take several minutes to retrain a port, and for the CLI to allow further command input.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre retraining
Console(config-if)#
```

Related Commands

lre datarate (29-26)

Downloaded from www.Manualslib.com manuals search engine

lre rate-adaption

This command enables automatic line rate adaptation, which can set the optimal transmission rate based on existing line conditions. Use the **no** form to disable this feature.

Syntax

[**no**] **lre rate-adaption**

Default Setting

Enabled

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to enable rate adaptation for all VDSL ports, or in interface mode to enable it for a specific VDSL port.
- The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaptation is enabled and the port links up, the switch will determine the optimal transmission rate for the current conditions, setting the rate within the bounds defined by the **lre datarate** command (page 29-26).
- When rate adaptation is enabled and the signal quality deteriorates on any line or the link is re-established after being dropped, that port will automatically enter retraining and connect at the optimum rate if **lre auto-retraining** (page 29-31) is enabled. Otherwise, the rate can be manually retrained using the **lre retraining** command (page 29-32).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre rate-adaption
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre datarate (29-26)
show lre rate-adaption (29-75)

lre apply

This command applies all global VDSL settings to each VDSL port on the switch or to a specified port, overwriting any previous settings configured for specific interfaces. Use the **no** form to restore the default setting.

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- Enter this command in global configuration mode to apply all configured global VDSL settings to all VDSL ports, or in interface mode to apply all settings for a specific VDSL port.
- Global configuration settings made with the **lre** commands are not applied to any interface until this command is entered.

Example

The following applies all global VDSL settings to Port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lre apply
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Line Profile Commands

This section describes how to configure a list of communication parameters such as data rates and acceptable noise margins which can be applied to all VDSL ports or to a selected group of ports.

Table 29-7 Line Profile Commands

Command	Function	Mode	Page
line-profile	Enters VDSL Line Profile configuration mode	GC	29-36
lre line-profile	Applies a line profile to selected VDSL ports	GC/IC	29-37
band-plan	Sets the frequency bands used for VDSL signals	VLP*	29-38
option-band	Sets the frequencies to be used for the optional US0 band.	VLP	29-39
ham-band	Sets the HAM radio band that will be blocked to VDSL signals based on defined frequencies	VLP	29-40
region-ham-band	Sets the HAM radio band that will be blocked to VDSL signals based on defined usage types	VLP	29-41
tone	Disables VDSL signals at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz	VLP	29-42
max-power	Sets the maximum aggregate downstream or upstream power	VLP	29-43
min-protection	Configures the minimum level of impulse noise protection for all bearer channels	VLP	29-44
channel	Sets the channel mode to fast or interleaved	VLP	29-45
down-max-inter-delay up-max-inter-delay	Sets the maximum interleave delay on a downstream/upstream channel	VLP	29-46

Downloaded from www.Manualslib.com manuals search engine

Table 29-7 Line Profile Commands

Command	Function	Mode	Page
down-fast-max-datarate down-fast-min-datarate up-fast-max-datarate up-fast-min-datarate down-slow-max-datarate down-slow-min-datarate up-slow-max-datarate up-slow-min-datarate	Sets maximum/minimum data rate on a fast/slow downstream/upstream channel	VLP	29-47
down-target-noise-mgn up-target-noise-mgn	Sets the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization on a downstream/upstream channel	VLP	29-48
down-min-noise-mgn up-min-noise-mgn	Sets the minimum acceptable signal-to-noise margin on a downstream/upstream channel	VLP	29-49

* VDSL Line Profile configuration mode.

line-profile

This command enters VDSL Line Profile configuration mode.

Syntax

line-profile *profile-name*

profile-name – Name of the profile. (Range: 1-31 alphanumeric characters)

Command Mode

Global Configuration

Command Usage

All commands entered in this mode are stored under the named profile, and take effect only when this profile is applied to a set of VDSL ports.

Downloaded from www.Manualslib.com manuals search engine

Example

The following creates a VDSL line profile named southport.

```
Console(config)#line-profile southport
Console(config)#
```

Related Commands

show lre line-profile (29-77)

lre line-profile

This command applies a line profile to selected VDSL ports. Use the **no** form to restore the default settings for the selected ports.

Syntax

[**no**] **lre line-profile** *profile-name*

profile-name – Name of the profile. (Range: 1-31 alphanumeric characters)

Default Setting

The default profile as specified in RFC 3728.

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Command Usage

- First create a profile of VDSL configuration settings using the other commands described in this section, then enter Global Configuration mode to apply the profile to all VDSL ports on the switch using the **lre line-profile** command. Or use the **interface** command to select a specific port, and then use the **lre line profile** command to apply the settings to that interface.
- The default profile includes all the system default settings for VDSL lines, and can specified by entering the **no lre line-profile** command.

Downloaded from www.Manualslib.com manuals search engine

Example

The following applies the line profile named southport to all VDSL ports.

```
Console(config)#lre line-profile southport
Console(config)#
```

band-plan

This command sets the frequency bands used for VDSL signals based on a set of predefined plans. Use the **no** form to restore the default status.

Syntax

band-plan *value*
no band-plan

value – Index for a predefined band plan.
(See Table 29-3, "VDSL2 Band Plans," on page 29-5.)

Default Setting

5 (100/100)

Command Mode

VDSL Line Profile

Command Usage

The band plan options provided by this command are listed in Table 29-3, "VDSL2 Band Plans," on page 29-5. The first field in the band plan designator indicates the ITU standard, the second field indicates the lower frequency bound, and the third field indicates the upper frequency bound. The band plans are also described by ITU-T Standards G.9932.

Example

This example sets the band plan to 998-640-30000.

```
Console(config-line-profile)#band-plan 5
Console(config-line-profile)#
```

Related Commands

lre band-plan (29-4)

Downloaded from www.Manualslib.com manuals search engine

option-band

This command sets the frequencies to be used for optional Upstream Band 0 (US0). Use the **no** form to restore the default status.

Syntax

option-band *value*
no option-band

value – Index of predefined frequency bounds for US0.
(Options:0 - No optional band
1 - ITU-T G993.2, Annex A, 6-32, 26-138 kHz
2 - ITU-T G993.2, Annex B, 32-64, 138-276 kHz
3 - ITU-T G993.2, Annex B, 6-64, 26-276 kHz

Default Setting

0 (No optional band)

Command Mode

VDSL Line Profile

Command Usage

Performance enhancements have been incorporated in G.993.2 for the optional US0 band (specifically, support in initialization for training of time domain equalizers and echo cancellers) which provide more reliable operation.

Example

This example sets configures the frequency bounds for US0 to 6-32 KHz.

```
Console(config-line-profile)#option-band 2
Console(config-line-profile)#
```

Related Commands

lre option-band (29-6)

Downloaded from www.Manualslib.com manuals search engine

ham-band

This command sets the Handheld Amateur Radio (HAM) band that will be blocked to VDSL signals based on defined frequencies. Use the **no** form to restore the default status.

Syntax

ham-band *value*
no ham-band

value – HAM band mask.
(See Table 29-4, "HAM Band Notches," on page 29-7.)

Default Setting

22 (none)

Command Mode

VDSL Line Profile

Command Usage

Using a HAM band mask prevents interference with other systems (e.g., amateur radio) that use narrow band transmission in the VDSL frequency band. The selected frequency range will not be used to transmit data on the VDSL line. You may need to specify a mask if required by local regulations or if specific incidents of interference are reported within a service area.

Example

This example sets a HAM band notch in the transmitted power spectrum in the 10.000 - 10.150 MHz transmission band (also called the 30 meter band).

```
Console(config-line-profile)#ham-band 11
Console(config-line-profile)#
```

Related Commands

region-ham-band (29-41)
lre ham-band (29-7)

Downloaded from www.Manualslib.com manuals search engine

region-ham-band

This command sets the ham radio band that will be blocked to VDSL signals based on defined usage types. Use the **no** form to restore the default status.

Syntax

region-ham-band *value*
no region-ham-band

value – HAM band mask for designated usage type.
(See Table 29-5, "HAM Band Notches for Usage Types," on page 29-10.)

Default Setting

36 (none)

Command Mode

VDSL Line Profile

Command Usage

Using a HAM band mask prevents interference with other systems (e.g., amateur radio) that use narrow band transmission in the VDSL frequency band. The selected frequency range will not be used to transmit data on the VDSL line. You may need to specify a mask if required by local regulations or if specific incidents of interference are reported within a service area.

Example

This example sets a HAM band notch in the transmitted power spectrum to avoid interference with CB radios.

```
Console(config-line-profile)#region-ham-band 34
Console(config-line-profile)#
```

Related Commands

ham-band (29-40)
lre region-ham-band (29-9)

Downloaded from www.Manualslib.com manuals search engine

tone

This command disables VDSL signals at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz. Use the **no** form to restore the default setting.

Syntax

lre tone {**tx** | **rx**} *value*
no lre tone {**tx** | **rx**}

- **tx** – Downstream band plan.
- **rx** – Upstream band plan.
- *value* – Index of low-end frequency range to disable.
  (Options:1 - all tones on
  2 - disable tones at 640 KHz and below
  3 - disable tones at 1.1 MHz and below
  4 - disable tones at 2.2 MHz and below)

Default Setting

3 (disable tones at 1.1 MHz and below)

Command Mode

VDSL Line Profile

Command Usage

- This command specifies a frequency beneath which VDSL signals are not allowed. For example, the default lower frequency bound for DS1 defined in Annex C of G.993.2 is 640 KHz. The low-end frequencies filtered out by this command are used for common POTS or ISDN services.
- The frequency bound specified by this command takes precedence over that defined in the selected band plan (see **band-plan**, page 29-38).

Downloaded from www.Manualslib.com manuals search engine

Example

The following disables all tone beneath 640 kHz on the upstream band plan.

```
Console(config-line-profile)#tone tx 2
Console(config-line-profile)#
```

Related Commands

lre tone (29-21)

max-power

This command sets the maximum aggregate downstream or upstream power. Use the **no** form to restore the default setting.

Syntax

max-power {**down** | **up**} *value*
no max-power {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Maximum aggregate power. (Range: 0-255, in units of 0.25 dBm)

Default Setting

255 (63.75 dBm)

Command Mode

VDSL Line Profile

Example

The following sets the maximum downstream power to 14.5 dBm.

```
Console(config-line-profile)#max-power down 58
Console(config-line-profile)#
```

Related Commands

lre max-power (29-22)

Downloaded from www.Manualslib.com manuals search engine

min-protection

This command configures the minimum level of impulse noise protection for all bearer channels. Use the **no** form to restore the default setting.

Syntax

min-protection {**down** | **up**} *value*
no max-power {**down** | **up**}

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – The number of consecutive DMT symbols for which errors can be completely corrected. (Range: 0-255, in units of 0.5 DMT symbols, or 125 microseconds)

Default Setting

0

Command Mode

VDSL Line Profile

Command Usage

- This minimum margin indicates the amount of increase in impulse noise that the system can tolerate under operational conditions while still ensuring required transmission quality.
- This command is used to set the time span of impulse noise protection, as seen at the input to the de-interleaver, for which errors can be completely corrected by the error correcting code, regardless of the number of errors within the errored DMT symbols.
- Note that this parameter only applies to interleaved channels. Refer to ITU-T G.993.2 for a full description of the methods used to calculate the minimum level of impulse noise protection.

Example

```
Console(config-line-profile)#min-protection down 5
Console(config-line-profile)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre min-protection (29-23)

channel

This command sets the channel mode to fast or interleaved. Use the **no** form to restore the default status.

Syntax

channel *mode*
no channel

mode – Channel mode (Options: fast, interleave)

Default Setting

interleaved

Command Mode

VDSL Line Profile

Command Usage

- Interleaving protects data against bursts of errors by using the Reed-Solomon error correction algorithm to spread the errors over a number of code words. A greater degree of interleaving provides more protection against noise pulses, but increases transmission delay and reduces the effective bandwidth.
- For applications that cannot tolerate latency (for example, voice), use the fast mode to disable the interleaving burst error correction method.

Example

```
Console(config-line-profile)#channel interleave
Console(config-line-profile)#
```

Related Commands

down/up-max-inter-delay (29-46)
lre channel (29-24)

Downloaded from www.Manualslib.com manuals search engine

down/up-max-inter-delay

These commands set the maximum interleave delay on a downstream/ upstream channel. Use the **no** form to restore the default settings to the profile.

Syntax

{down|up}-max-inter-delay *value*
no {down|up}-max-inter-delay

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Maximum interleave delay. (Range: 0-40, indicating units of 0.5 ms)

Default Setting

4 (2 ms)

Command Mode

VDSL Line Profile

Command Usage

- Interleaving causes a delay in the transmission of data.
- Setting the interleave delay to a value of zero disables interleaving.
- Interleave delay applies only to the interleave (slow) channel and defines the mapping (relative spacing) between subsequent input bytes at the interleaver input and their placement in the bit stream at the interleaver output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream allowing for improved impulse noise immunity at the expense of payload latency.

Example

This example sets the interleave delay on downstream channels to 3 milliseconds.

```
Console(config-line-profile)#down-max-inter-delay 6
Console(config-line-profile)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre interleave-max-delay (29-25)

down/up-fast/slow-max/min-datarate

These commands set the maximum/minimum data rate on a fast/slow downstream/upstream channel. Use the **no** form to restore the default settings to the profile.

Syntax

{down|up}-{fast|slow}-{max|min}-datarate *value*
no {down|up}-{fast|slow}-{max|min}-datarate

- **down** – Downstream bands.
- **up** – Upstream bands.
- **slow** – Slow (interleaved) channel.
- **fast** – Fast channel.
- **max** – Maximum channel data rate.
- **min** – Minimum channel data rate.
- *value* – The data rate. (Range: 1-200,000 kbps)

Default Setting

Maximum data rate: 200,000 kbps
Minimum data rate: 64 kbps

Command Mode

VDSL Line Profile

Command Usage

The command sets the minimum and maximum data rates supported by each upstream and downstream band. Bounding data rates should be set for both fast and slow channels if operation may sometimes disable or enable interleaving.

Downloaded from www.Manualslib.com manuals search engine

Example

The following sets the minimum and maximum data rates for the downstream fast channel on port 1.

```
Console(config-line-profile)#down-fast-max-datarate 190000
Console(config-line-profile)#down-fast-min-datarate 640
Console(config-line-profile)#
```

Related Commands

lre datarate (29-26)

down/up-target-noise-mgn

These commands set the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization on a downstream/upstream channel. Use the **no** form to restore the default settings.

Syntax

{**down**|**up**}-**target-noise-mgn** *value*
no {**down**|**up**}-**target-noise-mgn**

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Signal-to-noise margin. (Range: 0-62, in units of 0.5 dB)

Default Setting

12 dB

Command Mode

VDSL Line Profile

Command Usage

This command sets the noise margin that transceivers must achieve with a Bit Error Rate (BER) of 10^{-7} or better to successfully complete initialization. It indicates the maximum amount by which the reference crosstalk noise level can be increased during a BER test without causing the modem to fail the BER requirement.

Downloaded from www.Manualslib.com manuals search engine

Example

The following sets an SNR of 12 dB for the downstream channels and 18 dB for the upstream channels.

```
Console(config-line-profile)#down-target-noise-mgn 12
Console(config-line-profile)#up-target-noise-mgn 18
Console(config-line-profile)#
```

Related Commands

lre noise-mgn target (29-28)

down/up-min-noise-mgn

These commands set the minimum acceptable signal-to-noise margin on a downstream/upstream channel. Use the **no** form to restore the default settings.

Syntax

{down|up}-min-noise-mgn *value*
no {down|up}-min-noise-mgn

- **down** – Downstream bands.
- **up** – Upstream bands.
- *value* – Signal-to-noise margin. (Range: 0-62, in units of 0.5 dB)

Default Setting

10 dB

Command Mode

VDSL Line Profile

Command Usage

- This command sets the minimum noise margin the receiver can tolerate. If the noise margin falls below this level, the receiver will ask the sender to increase its transmit power. If it is not possible to increase the transmit power, a loss-of-margin defect occurs, the link will fail and the receiver will attempt to re-initialize.

Downloaded from www.Manualslib.com manuals search engine

- When rate adaptation is enabled (see Command Usage, page 29-32), the signal-to-noise ratio (SNR) is an indicator of link quality. The switch itself has no internal functions to ensure link quality. To ensure a stable link, you should add a margin to the theoretical minimum signal-to-noise ratio (SNR).

Example

The following sets the minimum noise margin on downstream channels to 12 dB.

```
Console(config-line-profile)#down-min-noise-mgn 12
Console(config-if)#
```

Related Commands

down/up-target-noise-mgn (29-48)
lre noise-mgn min (29-29)

Downloaded from www.Manualslib.com manuals search engine

Alarm Profile Commands

This section describes how to configure a list of threshold values for error states which can be applied all VDSL ports or to a selected group of ports.

Table 29-8 Alarm Profile Commands

Command	Function	Mode	Page
alarm-profile	Enters VDSL Line Alarm configuration mode	GC	29-52
lre alarm-profile	Applies an alarm profile to selected VDSL ports	GC/IC	29-52
init-failure	Sets threshold for initialization failures in the past 15 minutes	VAP*	29-53
thresh-15min-ess†	Sets threshold for Errored Seconds in the past 15 minutes	VAP	29-54
thresh-15min-lofs	Sets threshold for Loss of Framing in the past 15 minutes	VAP	29-55
thresh-15min-lols	Sets threshold for Loss of Link in the past 15 minutes	VAP	29-56
thresh-15min-loss	Sets threshold for Loss of Signal in the past 15 minutes	VAP	29-57
thresh-15min-lprs	Sets threshold for Loss of Power in the past 15 minutes	VAP	29-58
thresh-15min-sess	Sets threshold for Severely Errored Seconds in the past 15 minutes	VAP	29-59
thresh-15min-uass	Sets threshold for Unavailable Seconds in the past 15 minutes	VAP	29-60

* VDSL Alarm Profile configuration mode.

† When these thresholds are exceeded, notification messages are sent to registered SNMP hosts as required by RFC 3728, reported to the syslog system, and displayed on the console interface.

Downloaded from www.Manualslib.com manuals search engine

alarm-profile

This command enters VDSL Alarm Profile configuration mode. Use the **no** form to delete an alarm profile.

Syntax

[**no**] **alarm-profile** *profile-name*

profile-name – Name of the profile. (Range: 1-31 alphanumeric characters)

Command Mode

Global Configuration

Command Usage

All commands entered in this mode are stored under the named profile, and take effect only when this profile is applied to a set of VDSL ports.

Example

The following creates a VDSL alarm profile named southport.

```
Console(config)#alarm-profile southport
Console(config-alarm-profile)#
```

Related Commands

show lre alarm-profile (29-78)

lre alarm-profile

This command applies a line profile to selected VDSL ports. Use the **no** form to restore the default settings for the selected ports.

Syntax

[**no**] **lre alarm-profile** *profile-name*

profile-name – Name of the profile. (Range: 1-31 alphanumeric characters)

Command Mode

Global Configuration
Interface Configuration (VDSL Port)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

First create a profile of VDSL alarm thresholds using the other commands described in this section, then enter Global Configuration mode to apply the profile to all VDSL ports on the switch using the **lre alarm-profile** command. Or use the **interface** command to select a specific port, and then use the **lre alarm-profile** command to apply the settings to that interface.

Example

The following applies the alarm profile named southport to all VDSL ports.

```
Console(config)#lre alarm-profile southport
Console(config)#
```

init-failure

This command sets the threshold for initialization failures that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

init-failure *value*

value – Threshold for initialization failures.
(Range: 0-900 seconds; 0 disables the threshold)

Default Setting

1

Command Mode

VDSL Alarm Profile

Command Usage

- There are many factors which can cause an initialization failure, including lossOfFraming, lossOfSignal, lossOfPower, lossOfSignalQuality, lossOfLink, dataInitFailure, configInitFailure, protocolInitFailure, or noPeerVtuPresent. All outstanding error conditions associated with a VDSL transceiver are defined by the vdslPhysCurrStatus bitmask in RFC 3728. However, note that since

Downloaded from www.Manualslib.com manuals search engine

the status of remote transceivers is obtained via the embedded operation channel (EOC), this information may be unavailable for units that are unreachable via the EOC during a line error condition. Therefore, not all conditions may always be included in its current status.

- This command sets the threshold for the number of initialization failures within any 15 minute collection interval for performance data. If the number of initialization failures in a particular 15-minute collection interval reaches or exceeds this value, a vdslInitFailureNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the initialization failure threshold to 5.

```
Console(config-alarm-profile)#init-failure 5
Console(config-alarm-profile)#
```

thresh-15min-ess

This command sets the threshold for Errored Seconds (ESs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-ess *value*

value – Threshold for Errored Seconds.
(Range: 0-900 seconds; 0 disables the threshold)

Default Setting

2

Command Mode

VDSL Alarm Profile

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- An Errored Second is a one-second interval containing one or more CRC anomalies, or one or more Loss of Signal (LOS) or Loss of Framing (LOF) defects.
- This command sets the threshold for the number of errored seconds within any 15 minute collection interval for performance data. If the number of errored seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfESsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the ESs threshold to 25.

```
Console(config-alarm-profile)#thresh-15min-ess 25
Console(config-alarm-profile)#
```

thresh-15min-lofs

This command sets the threshold for Loss of Frame seconds (LOFs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-lofs *value*

value – Threshold for Loss of Framing, or the number of seconds during which there was loss of framing in the indicated time interval. (Range: 0-900 seconds; 0 disables the threshold)

Default Setting

10

Command Mode

VDSL Alarm Profile

Downloaded from www.Manualslib.com manuals search engine

Command Usage

This command sets the threshold for the number of seconds during which there is loss of framing within any 15 minute collection interval for performance data. If loss of framing in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLofsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the LOFs threshold to 15.

```
Console(config-alarm-profile)#thresh-15min-lofs 15
Console(config-alarm-profile)#
```

thresh-15min-lols

This command sets the threshold for Loss of Link seconds (LOLs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-lols *value*

value – Threshold for Loss of Link, or the number of seconds during which there was loss of link in the indicated time interval. (Range: 0-900 seconds; 0 disables the threshold)

Default Setting

10

Command Mode

VDSL Alarm Profile

Command Usage

This command sets the threshold for the number of seconds during which there is loss of link within any 15 minute collection interval for performance data. If loss of link in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLolsThreshNotification

Downloaded from www.Manualslib.com manuals search engine

notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the LOLs threshold to 15.

```
Console(config-alarm-profile)#thresh-15min-lols 15
Console(config-alarm-profile)#
```

thresh-15min-loss

This command sets the threshold for Loss of Signal seconds (LOSs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-loss *value*

value – Threshold for Loss of Signal, or the number of seconds during which there was loss of signal in the indicated time interval. (Range: 0-900 seconds; 0 disables the threshold)

Default Setting

2

Command Mode

VDSL Alarm Profile

Command Usage

This command sets the threshold for the number of seconds during which there is loss of signal within any 15 minute collection interval for performance data. If loss of signal in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLossThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Downloaded from www.Manualslib.com manuals search engine

Example

The following sets the LOSs threshold to 15.

```
Console(config-alarm-profile)#thresh-15min-loss 15
Console(config-alarm-profile)#
```

thresh-15min-lprs

This command sets the threshold for Loss of Power Seconds (LPRs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-lprs *value*

value – Threshold for Loss of Power Seconds.
(Range: 0-900 seconds; 0 disables the threshold)

Default Setting

10

Command Mode

VDSL Alarm Profile

Command Usage

This command sets the threshold for the number of loss of power seconds within any 15 minute collection interval for performance data. If the number of loss of power seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfLprsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the LPRs threshold to 15.

```
Console(config-alarm-profile)#thresh-15min-lprs 15
Console(config-alarm-profile)#
```


Downloaded from www.Manualslib.com manuals search engine

thresh-15min-sess

This command sets the threshold for Severely Errored Seconds (SESs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-sess *value*

value – Threshold for Severely Errored Seconds. (Range: 0-900 seconds; 0 disables the threshold)

Default Setting

2

Command Mode

VDSL Alarm Profile

Command Usage

- A Severely Errored Second is a one-second interval containing 18 or more CRC-8 anomalies, one or more Loss of Signal (LOS) defects, one or more Severely Errored Frame (SEF) defects, or one or more Loss of Power (LPR) defects.
- This command sets the threshold for the number of severely errored seconds within any 15 minute collection interval for performance data. If the number of severely errored seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfSESsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the SESs threshold to 15.

```
Console(config-alarm-profile)#thresh-15min-sess 15
Console(config-alarm-profile)#
```


Downloaded from www.Manualslib.com manuals search engine

thresh-15min-uass

This command sets the threshold for Unavailable Seconds (UASs) that can occur within any given 15 minutes. Use the **no** form to restore the default setting.

Syntax

thresh-15min-uass *value*

value – Threshold for Unavailable Seconds.
(Range: 0-900 seconds; 0 disables the threshold)

Default Setting

10

Command Mode

VDSL Alarm Profile

Command Usage

- An Unavailable Seconds is a one-second interval during which the VDSL transceiver is powered up but not available (i.e., not in the Showtime state). A VDSL line will become unavailable at the onset of 10 contiguous Severely Errored Seconds. Once unavailable, the line should become available at the onset of 10 contiguous seconds with no SESs.
- This command sets the threshold for the number of severely errored seconds within any 15 minute collection interval for performance data. If the number of severely errored seconds in a particular 15-minute collection interval reaches or exceeds this value, a vdslPerfUASsThreshNotification notification will be generated. (Refer to RFC 3728 for information on this notification message.) No more than one notification will be sent per interval.

Example

The following sets the UASs threshold to 15.

```
Console(config-alarm-profile)#thresh-15min-uass 15
Console(config-alarm-profile)#
```


Downloaded from www.Manualslib.com manuals search engine

Displaying VDSL Information

This section describes the commands used to display information on VDSL configuration settings, signal status, and communication statistics.

Table 29-9 Commands for Displaying VDSL Information

Command	Function	Mode	Page
Displaying Configuration Settings			
show lre band-plan	Displays the frequency bands used for VDSL signals	PE	29-62
show lre option-band	Displays the frequencies to be used for the optional US0 band	PE	29-63
show lre ham-band	Displays the HAM radio band that is blocked to VDSL signals based on defined frequencies	PE	29-64
show lre region-ham-band	Displays the HAM radio band that is blocked to VDSL signals based on defined usage types	PE	29-65
show lre psd	Displays the power level set for each of the PSD breakpoints	PE	29-67
show lre psd-mask-level	Displays the predefined PSD mask configured for an interface	PE	29-68
show lre pbo-config	Displays the mask used to reduce the power spectral density (PSD) of transmitted signals at specified frequency breakpoints	PE	29-69
show lre upbo	Shows if upstream power backoff is enabled or disabled	PE	29-70
show lre tone	Shows if VDSL signals are enabled or disabled at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz	PE	29-71
show lre interleave-max-delay	Displays the maximum interleave-delay for downstream and upstream channels	PE	29-72
show lre datarate	Displays the minimum and maximum data rate for downstream and upstream fast or slow (interleaved) channels	PE	29-73

Downloaded from www.Manualslib.com manuals search engine

Table 29-9 Commands for Displaying VDSL Information (Continued)

Command	Function	Mode	Page
show lre noise-mgn	Displays the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization	PE	29-74
show lre rate-adaption	Shows if line rate adaptation which sets the optimal transmission rate based on existing line conditions is enabled or disabled	PE	29-75
show lre config	Shows the VDSL configuration settings for an interface	PE	29-76
show lre line-profile	Displays a specified line profile which may be applied selected VDSL ports	PE	29-77
show lre alarm-profile	Displays a specified alarm profile which may be applied selected VDSL ports	PE	29-78
Displaying System Status			
show lre	Displays the communication status of the VDSL line	PE	29-79
show lre phys-info	Displays physical layer information about the VDSL line	PE	29-80
show lre rate-info	Displays rate information for the VDSL line	PE	29-81
Displaying Statistics			
show lre perf	Displays performance information including common error conditions over predefined intervals for the VDSL line	PE	29-82

show lre band-plan

This command displays the frequency bands used for VDSL signals.

Syntax

show lre band-plan [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Use this command without the interface parameter to display the band plans used for all VDSL ports on the switch, or with an interface to display the band plan used for a specific port.
- The band plan options provided by this switch are described by ITU-T Standards G.997 and G.998. The first field in the band plan designator indicates the ITU standard, the second field indicates the lower frequency bound, and the third field indicates the upper frequency bound.
- A list of predefined band plans are shown in Table 29-3, "VDSL2 Band Plans," on page 29-5.

Example

This example shows that the band plan for Port 1 is based on ITU-T G.998, the frequency bounds are 64 kHz to 30 MHz, and the data rate is symmetric.

```
Console#show lre band-plan 1/1
    Bandplan :                              998-640-30000 100/100

Console#
```

Related Commands

lre band-plan (29-4)

show lre option-band

This command displays the frequencies to be used for the optional US0 band.

Syntax

show lre option-band [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Use this command without the interface parameter to display the optional US0 band used for all VDSL ports on the switch, or with an interface to display the optional band used for a specific port.
- Refer to the **lre option-band** command on page 29-6 for a list of the frequency bounds for the optional band supported by this switch.

Example

This example shows that the optional US0 band used for Port 1.

```
Console#show lre option-band 1/1
    Optional Band :                          Annex A  6-32 26 to 138
kHz
Console#
```

Related Commands

lre option-band (29-6)

show lre ham-band

This command displays the HAM radio band that is blocked to VDSL signals based on defined frequencies.

Syntax

show lre ham-plan [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to display the HAM band frequency filter used for all VDSL ports on the switch, or with an interface to display the filter used for a specific port.
- Refer to **Table 29-4, "HAM Band Notches," on page 29-7** for a list of the stop bands for HAM radio frequencies supported by this switch.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows that the HAM band in the 1.810 - 1.825 MHz range is blocked to VDSL signals for Port 1.

```
Console#sh lre ham-band 1/1
    RFI-BAND01: 1.810 - 1.825 MHz: ANNEX F :                    ON
    RFI-BAND02: 1.810 - 2.000 MHz: ETSI, T1E1 :                 OFF
    RFI-BAND03: 1.9075 - 1.9125 MHz: ANNEX F :                  OFF
    RFI-BAND04: 3.500 - 3.575 MHz: ANNEX F :                    OFF
    RFI-BAND05: 3.500 - 3.800 MHz: ETSI :                       OFF
    RFI-BAND06: 3.500 - 4.000 MHz: T1E1 :                       OFF
    RFI-BAND07: 3.747 - 3.754 MHz: ANNEX F :                    OFF
    RFI-BAND08: 3.791 - 3.805 MHz: ANNEX F :                    OFF
    RFI-BAND09: 7.000 - 7.100 MHz: ANNEX F, ETSI :              OFF
    RFI-BAND10: 7.000 - 7.300 MHz: T1E1:                        OFF
    RFI-BAND11: 10.100 - 10.150 MHz: ANNEX F, ETSI, T1E1:       OFF
    RFI-BAND12: 14.000 - 14.350 MHz: ANNEX F, ETSI, T1E1:       OFF
    RFI-BAND13: 18.068 - 18.168 MHz: ANNEX F, ETSI, T1E1:       OFF
    RFI-BAND14: 1.800 - 1.825 MHz: HAM Band 1:                  OFF
    RFI-BAND15: 3.500 - 3.550 MHz: HAM Band 2:                  OFF
    RFI-BAND16: 3.790 - 3.800 MHz: HAM Band 3:                  OFF
    RFI-BAND17: 1.800 - 1.810 MHz: RFI Notch:                   OFF
    RFI-BAND18: 21.000 - 21.450 MHz: ANNEX F, ETSI, T1E1:       OFF
    RFI-BAND19: 24.890 - 24.990 MHz: ANNEX F, ETSI, T1E1:       OFF
    RFI-BAND20: 28.000 - 29.100 MHz: ANNEX F, ETSI, T1E1:       OFF
    RFI-BAND21: 28.000 - 29.700 MHz: ANNEX F, ETSI, T1E1:       OFF
Console#
```

Related Commands

lre ham-band (29-7)

show lre region-ham-band

This command displays the HAM radio band that is blocked to VDSL signals based on defined usage types.

Syntax

show lre region-ham-band [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Use this command without the interface parameter to display the HAM band usage filter used for all VDSL ports on the switch, or with an interface to display the filter used for a specific port.
- Refer to **Table 29-5, "HAM Band Notches for Usage Types," on page 29-10** for a list of the stop bands for radio usage types supported by this switch.

Example

This example shows that the amateur radio band in the 1.800 - 2.000 MHz range is blocked to VDSL signals for Port 1.

```
Console#show lre region-ham-band 1/1
    RFI-BAND01: OFF 1.800 - 2.000 MHz: Amateur Radio:           ON
    RFI-BAND02: 2.173 - 2.191 MHz: GMDSS:                       OFF
    RFI-BAND03: 2.850 - 3.155 MHz: Aeronautical Comm.:          OFF
    RFI-BAND04: 3.400 - 3.500 MHz: Aeronautical Comm.:          OFF
    RFI-BAND05: 3.500 - 3.800 MHz: Amateur Radio:               OFF
    RFI-BAND06: 3.800 - 4.000 MHz: Aeronautical/Broadcasting:   OFF
    RFI-BAND07: 4.200 - 4.215 MHz: GMDSS:                       OFF
    RFI-BAND08: 4.650 - 4.850 MHz: Aeronautical Comm.:          OFF
    RFI-BAND09: 5.450 - 5.730 MHz: Aeronautical Comm.:          OFF
    RFI-BAND10: 5.900 - 6.200 MHz: DRM Radio:                   OFF
    RFI-BAND11: 6.300 - 6.320 MHz: GMDSS:                       OFF
    RFI-BAND12: 6.525 - 6.765 MHz: Aeronautical Comm.:          OFF
    RFI-BAND13: 7.000 - 7.200 MHz: Amateur Radio:               OFF
    RFI-BAND14: 7.200 - 7.450 MHz: DRM Radio:                   OFF
    RFI-BAND15: 8.405 - 8.420 MHz: GMDSS:                       OFF
    RFI-BAND16: 8.815 - 9.040 MHz: Aeronautical Comm.:          OFF
    RFI-BAND17: 9.400 - 9.900 MHz: DRM Radio:                   OFF
    RFI-BAND18: 10.005 - 10.100 MHz: Aeronautical Comm.:        OFF
    RFI-BAND19: 10.100 - 10.150 MHz: Amateur Radio:             OFF
    RFI-BAND20: 11.175 - 11.400 MHz: Aeronautical Comm.:        OFF
    RFI-BAND21: 11.600 - 12.100 MHz: DRM Radio:                 OFF
    RFI-BAND22: 12.570 - 12.585 MHz: GMDSS:                     OFF
    RFI-BAND24: 13.570 - 13.870 MHz: DRM Radio:                 OFF
    RFI-BAND25: 14.000 - 14.350 MHz: Amateur Radio:             OFF
    RFI-BAND26: 15.010 - 15.100 MHz: Aeronautical Comm.:        OFF
    RFI-BAND27: 15.100 - 15.800 MHz: DRM Radio:                 OFF
    RFI-BAND28: 16.795 - 16.810 MHz: GMDSS:                     OFF
    RFI-BAND29: 17.480 - 17.900 MHz: DRM Radio:                 OFF
    RFI-BAND30: 17.900 - 18.030 MHz: Aeronautical Comm.:        OFF
    RFI-BAND31: 18.068 - 18.168 MHz: Amateur Radio:             OFF
    RFI-BAND32: 21.000 - 21.450 MHz: Amateur Radio:             OFF
    RFI-BAND33: 24.890 - 24.990 MHz: Amateur Radio:             OFF
    RFI-BAND34: 26.965 - 27.405 MHz: CB Radio:                  OFF
    RFI-BAND35: 28.000 - 29.700 MHz: Amateur Radio:             OFF
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre region-ham-band (29-9)

show lre psd

This command displays the power level set for each of the PSD breakpoints.

Syntax

show lre psd [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to display the PSD used for all VDSL ports on the switch, or with an interface to display it used for a specific port.
- The Power Spectral Density (PSD) defines the power spectrum used over all of the VDSL upstream and downstream channels. It is configured using the **lre psd-breakpoints** command (page 29-12), **lre psd-frequencies** command (page 29-13), and **lre psd-value** command (page 29-15).

Example

This example shows that the default PSD is set at -12 dBm/Hz for all of the breakpoints for Port 1. No slopes at the bounding frequencies nor peaks at the center frequency for any band has been configured.

```
Console#show lre psd 1/1
    138 kHz :                              -12 dBm/Hz
    640 kHz :                              -12 dBm/Hz
    648 kHz :                              -12 dBm/Hz
    1100 kHz :                              -12 dBm/Hz
    1108 kHz :                              -12 dBm/Hz
    2000 kHz :                              -12 dBm/Hz
    2008 kHz :                              -12 dBm/Hz
```


Downloaded from www.Manualslib.com manuals search engine

```
    3000 kHz :                              -12 dBm/Hz
    3008 kHz :                              -12 dBm/Hz
    3750 kHz :                              -12 dBm/Hz
    3758 kHz :                              -12 dBm/Hz
    4500 kHz :                              -12 dBm/Hz
    4508 kHz :                              -12 dBm/Hz
    5200 kHz :                              -12 dBm/Hz
    5208 kHz :                              -12 dBm/Hz
    7000 kHz :                              -12 dBm/Hz
    7008 kHz :                              -12 dBm/Hz
    8500 kHz :                              -12 dBm/Hz
    8508 kHz :                              -12 dBm/Hz
    12000 kHz :                              -12 dBm/Hz
    12008 kHz :                              -12 dBm/Hz
    16700 kHz :                              -12 dBm/Hz
    16708 kHz :                              -12 dBm/Hz
    16708 kHz :                              -12 dBm/Hz
    17600 kHz :                              -12 dBm/Hz
    17608 kHz :                              -12 dBm/Hz
    18100 kHz :                              -12 dBm/Hz
    18108 kHz :                              -12 dBm/Hz
    30000 kHz :                              -12 dBm/Hz
Console#
```

Related Commands

lre psd-breakpoints (29-12)
lre psd-frequencies (29-13)
lre psd-value (29-15)

show lre psd-mask-level

This command displays the predefined PSD mask configured for an interface.

Syntax

show lre psd-mask-level [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Use this command without the interface parameter to display the predefined PSD mask used for all VDSL ports on the switch, or with an interface to display it used for a specific port.
- Refer to **Table 29-6, "PSD Mask Options," on page 29-17** for a list of the PSD mask options supported by this switch.

Example

This example shows that the PSD mask defined in Annex F of ITU-T G.993.1 is being used for Port 1.

```
Console#show lre psd-mask-level 1/1
    PSD Mask Level :                        ANNEX F
Console#
```

Related Commands

lre psd-mask-level (29-16)

show lre pbo-config

This command displays the mask used to reduce the power spectral density (PSD) of transmitted signals at specified frequency breakpoints.

Command Mode

Privileged Exec

Command Usage

- Upstream power back-off (UPBO) is used to mitigate far-end crosstalk caused by upstream transmissions from shorter to longer loops, thereby ensuring that the upstream signals passing between short to long loops are compatible.
- The **lre pbo-config** command (page 29-18) is used to reshape the PSD by reducing the power spectral density (PSD) of transmitted signals at specified frequency breakpoints. (Note that the breakpoint frequencies are expressed in units or 1000 decibels.)

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows that the UPBO mask used for all upstream traffic.

```
Console#show lre pbo-config
CO Rx PSD constants
    K1[0] = 0, K1[1] = -60000, K1[2] = -60000
    K1[3] = -60000, K1[4] = 0, K1[5] = 0
CO Tx PSD constants
    K2[0] = 0, K2[1] = -11200, K2[2] = -7419
    K2[3] = -7419, K2[4] = 0, K2[5] = 0

Console#
```

Related Commands

lre pbo-config (29-18)

show lre upbo

This command shows if upstream power backoff is enabled or disabled.

Syntax

show lre upbo [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to display the UPBO status used for all VDSL ports on the switch, or with an interface to display it used for a specific port.
- If UPBO is enabled by the **lre upbo** command (page 29-19), the upstream power backoff PSD mask will be applied to the specified ports based on configuration settings specified by the **lre pbo-config** command (page 29-18) as described in ITU-T G.992.2.
- If UPBO is enabled, and a PBO mask has been defined, the transceiver will use the PBO mask to control upstream power backoff. If UPBO is enabled, but a PBO mask has not been configured, the specified

Downloaded from www.Manualslib.com manuals search engine

transceiver will automatically control upstream power backoff based on default values set by the DSP engine.

Example

This example shows that UPBO has been enabled on Port 1.

```
Console#sh lre upbo 1/1
    UPBO status :                          Enable
Console#
```

Related Commands

lre upbo (29-19)

show lre tone

This command shows if VDSL signals are enabled or disabled at frequencies less than or equal to 640 KHz, 1.1 MHz or 2.2 MHz.

Syntax

show lre tone [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

Use this command without the interface parameter to show if VDSL signals are disabled at low-end frequencies for all VDSL ports on the switch, or with an interface to display this information for a specific port.

Example

This example shows the default setting for disabled low-end frequencies.

```
Console#show lre tone 1/1
    RX Bandplan Configuration :            Disable tones 1.1 MHz and below
    TX Bandplan Configuration :            Disable tones 1.1 MHz and below
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre tone (29-21)

show lre interleave-max-delay

This command displays the maximum interleave-delay that can be used for downstream and upstream channels.

Syntax

show lre interleave-max-delay [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to show the maximum interleave delay for all VDSL ports on the switch, or with an interface to display this information for a specific port.
- Interleave delay applies only to the interleave (slow) channel and defines the mapping (relative spacing) between subsequent input bytes at the interleaver input and their placement in the bit stream at the interleaver output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream allowing for improved impulse noise immunity at the expense of payload latency.

Example

This example shows the default settings for the maximum interleave delay.

```
Console#show lre interleave-max-delay 1/1
    Downstream InterleaveDelay Max:        2 ms
    Upsteam InterleaveDelay Max:           2 ms
Console#
```

Related Commands

lre interleave-max-delay (29-25)

Downloaded from www.Manualslib.com manuals search engine

show lre datarate

This command displays the minimum and maximum data rate for downstream and upstream fast or slow (interleaved) channels.

Syntax

show lre interleave-delay [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to show the data rate bounds for all VDSL ports on the switch, or with an interface to display this information for a specific port.
- No bounds are set for the slow channels by default. Bounding data rates should be set for both the fast and slow channels if operation may sometimes disable or enable interleaving

Example

This example shows the default data rate bounds.

```
Console#show lre datarate 1/1
    Downstream Datarate Fast Max :          200000 kbps
    Downstream Datarate Fast Min :          64 kbps
    Downstream Datarate Slow Max :          0 kbps
    Downstream Datarate Slow Min :          0 kbps
    Uptream Datarate Fast Max :             200000 kbps
    Uptream Datarate Fast Min :             64 kbps
    Uptream Datarate Slow Max :             0 kbps
    Uptream Datarate Slow Min :             0 kbps
Console#
```

Related Commands

lre datarate (29-26)

Downloaded from www.Manualslib.com manuals search engine

show lre noise-mgn

This command displays the targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization.

Syntax

show lre noise-mgn [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to show the SNR target for all VDSL ports on the switch, or with an interface to display this information for a specific port.
- Each transceiver must achieve the targeted noise margin with a Bit Error Rate (BER) of 10^{-7} or better to successfully complete initialization. This indicates the maximum amount by which the reference crosstalk noise level can be increased during a BER test without causing the modem to fail the BER requirement.

Example

This example shows the default noise margin targets.

```
Console#show lre noise-mgn 1/1
    Upstream Noise Margin Min:              5 dB
    Downstream Noise Margin Min:            5 dB
    Upstream Noise Margin Target:           6 dB
    Downstream Noise Margin Target:         6 dB
Console#
```

Related Commands

lre noise-mgn target (29-28)

Downloaded from www.Manualslib.com manuals search engine

show lre rate-adaption

This command shows if line rate adaptation which sets the optimal transmission rate based on existing line conditions is enabled or disabled.

Syntax

show lre rate-adaption [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

- Use this command without the interface parameter to show if rate adaptation has been enabled for all VDSL ports on the switch, or with an interface to display this information for a specific port.
- The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaption is enabled, the switch will determine the optimal transmission rate for the current conditions.

Example

This example shows the default setting for rate adaption.

```
Console#show lre rate-adaption 1/1
    Rate Adaption :                         Adaptive
Console#
```

Related Commands

Command Usage (29-32)

Downloaded from www.Manualslib.com manuals search engine

show lre config

This command shows the VDSL configuration settings for an interface.

Syntax

show lre config [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Command Usage

Use this command without the interface parameter to show the VDSL settings for all VDSL ports on the switch, or with an interface to display this information for a specific port.

Example

This example shows the VDSL configuration settings for Port 1.

```
Console#show lre config 1/1
    Link admin:                          Normal
    Auto Retraining:                     Enable
    Channel Mode :                       Interleave
    UPBO status :                        Enable
    Rate Adaption :                      Fixed
    Bandplan :                           998-640-30000 100/100
    Optional Band :                      No optional Band Selected
    PSD Mask Level :                     ANNEX F
    SNR Margin Min :                     20 dBm
    Transmit Power                       8.5 dBm
    Downstream Min Protection            0 usec
    Upstream Min Protection              0 usec
    Downstream Max Power                 63 dBm
    Upstream Max Power                   63 dBm
    Downstream InterleaveDelay Max:      2 ms
    Upsteam InterleaveDelay Max:         2 ms
    Upstream Noise Margin Min:           5 dB
    Downstream Noise Margin Min:         5 dB
    Upstream Noise Margin Target:        6 dB
    Downstream Noise Margin Target:      6 dB
    Downstream SNR Margin Target :       24 dBm
    Upstream SNR Margin Target :         32 dBm
    RX Bandplan Configuration :          Disable tones 1.1 MHz and below
    TX Bandplan Configuration :          Disable tones 1.1 MHz and below
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

lre apply (29-34)

show lre line-profile

This command displays a specified line profile which may be applied selected VDSL ports.

Syntax

show lre line-profile [*profile-name*]

profile-name – Name of the profile. (Range: 1-31 alphanumeric characters)

Command Mode

Privileged Exec

Command Usage

Use this command without a profile name to show the settings for all configured line profiles, or with a profile name to display the settings for a specific profile.

Example

This example shows the default settings for a line profile.

```
Console#show lre line-profile northport
northport:
    down-fast-max-datarate :0
    down-fast-min-datarate :0
    down-max-inter-delay :4
    down-min-noise-mgn :10
    down-slow-max-datarate :200000
    down-slow-min-datarate :64
    down-target-noice-mgn :12
    down-target-snr-mgn :24
    snr-min-margin :20
    up-fast-max-datarate :0
    up-fast-min-datarate :0
    up-max-inter-delay :4
    up-min-noice-mgn :10
    up-slow-max-datarate :200000
    up-slow-min-datarate :64
    up-target-noice-mgn :12
    up-target-snr-mgn :32
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

line-profile (29-36)
lre line-profile (29-37)

show lre alarm-profile

This command displays a specified alarm profile which may be applied selected VDSL ports.

Syntax

show lre alarm-profile [*profile-name*]

profile-name – Name of the profile. (Range: 1-31 alphanumeric characters)

Command Mode

Privileged Exec

Command Usage

Use this command without a profile name to show the settings for all configured alarm profiles, or with a profile name to display the settings for a specific profile.

Example

This example shows the default settings for an alarm profile.

```
Console#show lre alarm-profile northport
northport:
    threshold 15min ess                2 seconds
    threshold 15min sess               2 seconds
    threshold 15min lols              10 seconds
    threshold 15min lofs              10 seconds
    threshold 15min loss               2 seconds
    threshold 15min lprs              10 seconds
    threshold 15min uass              10 seconds
    initialization failure             5
Console#
```

Related Commands

alarm-profile (29-52)
lre alarm-profile (29-52)

Downloaded from www.Manualslib.com manuals search engine

show lre

This command displays the communication status of the VDSL line.

Syntax

show lre *unit/port*

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Example

```
Console#show lre 1/1
port 1 status :                                 port enable(provisioned)
port 1 status :                                 port activating
Downstream Training Margin:                     8.0 dB
Upstream Training Margin:                       9.1 dB
Downstream Line Protection (Slow Path):         0.0 DMT Symbols
Upstream Line Protection (Slow Path):           0.0 DMT Symbols
Downstream delay:                               1.9 ms
Upstream delay:                                 1.9 ms
Tx total power :                                7.7 dbm
FE Tx total power :                             6.0 dbm
VDSL Estimated Loop Length :                    16 ft
G.Hs Estimated Near End Loop Length :           5 ft
G.Hs Estimated Far End Loop Length :            0 ft
Current framing mode:                           0x80
Far end capabilities mask:                      0x00
SNR Margin:                                     5.3 dB
Attenuation:                                    16.8 dB
Avg SNR Margin:                                 6.3 dB
Avg SNR:                                        32.9 dB
Console#
```

Table 29-10 show lre - display description

Field	Description
port status	(1) Indicates if the port is administratively enabled or disabled. (2) Indicates the current initialization or operational status.
Training Margin	The targeted signal-to-noise margin that VDSL ports must achieve to successfully complete initialization (see **lre noise-mgn target**, page 29-28).

Downloaded from www.Manualslib.com manuals search engine

Table 29-10 show lre - display description (Continued)

Field	Description
Line Protection (Slow Path)	The minimum level of impulse noise protection for all bearer channels (see **lre min-protection**, page 29-23).
Downstream/Upstream delay	The maximum interleave delay (see **lre interleave-max-delay**, page 29-25).
Tx total power	The maximum aggregate transmit power over all signal bands for the specified interface.
FE Tx total power	The maximum transmit power used at the far end.
VDSL Estimated Loop Length	Estimated length of the VDSL connection; used to calculate power backoff.
G.Hs Estimated Loop Length	Estimated length of the VDSL connection; used for handshaking.
Current framing mode	Only Packet Transfer Mode (PTM) framing is used for VDSL lines.
Far end capabilities mask	The capabilities supported by the attached CPE.
SNR Margin	Current signal-to-noise margin
Attenuation	Amount of attenuation in signal strength
Avg SNR Margin	Average signal-to-noise margin above the SNR.
Avg SNR	Average signal-to-noise ratio.

show lre phys-info

This command displays physical layer information about the VDSL line.

Syntax

show lre phys-info *unit/port*

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show lre phys-info 1/1
port 1/1 Phys info:
Phys current line rate :                71680 kpbs
Phys current attainable rate :          72064 kpbs
Phys current output power :             7.7 dbm
Phys current atn :                      1.4 dbm

Console#
```

Table 29-11 show lre phys-info - display description

Field	Description
Phys current line rate	Current data rate in steps of 1000 bits/second.
Phys current attainable rate	Maximum currently attainable data rate in steps of 1000 bits/second.
Phys current output power	Measured total output power transmitted by this VDSL port.
Phys current atn	Measured difference in the total power transmitted by the peer VTU (VDSL Transceiver Unit) and the total power received by this VTU.

show lre rate-info

This command displays rate information for the VDSL line.

Syntax

show lre rate-info [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show lre rate-info 1/1
port 1 Rate informaition :
Downstream line rate:                    119040 kbps
Upstream line rate:                      115648 kbps
Fast Downstream payload rate:            0 kbps
Slow Downstream payload rate:            104960 kbps
Fast Upstream payload rate:              0 kbps
Slow Upstream payload rate:              101952 kbps
Downstream attainable payload rate:      110080 kbps
Downstream attainable line rate:         129664 kbps
Upstream attainable payload rate:        109696 kbps
Upstream attainable line rate:           124480 kbps
Console#
```

Table 29-12 show lre rate-info - display description

Field	Description
line rate	The downstream and upsteam line rate.
payload rate	The actual payload carried on the fast and interleaved channels.
attainable payload rate	The maximum attainable payload on the downstream and upstream channels.
attainable line rate	The maximum attainable line rate on the downstream and upstream channels

show lre perf

This command displays performance information including common error conditions over predefined intervals for the VDSL line.

Syntax

show lre perf [*unit*/*port*]

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

Use this command without the interface parameter to show performance information for all VDSL ports on the switch, or with an interface to display this information for a specific port. For a description of the displayed items, refer to the "Alarm Profile Commands" on page 29-51.

Example

```
Console#show lre perf 1/1
port 1 performance counters since last reset :
Loss of frame : 0               Loss of signal :        0
Loss of power : 0               Errored seconds :       17
Severely error seconds: 0       Unavaliable seconds :   0

port 1 performance counters in current 15min interval :
Loss of frame : 0               Loss of signal :        0
Loss of power : 0               Errored seconds :       4
Severely error seconds: 0       Unavaliable seconds :   0

port 1 performance counters in current 1day interval :
Loss of frame : 0               Loss of signal :        0
Loss of power : 0               Errored seconds :       13
Severely error seconds: 0       Unavaliable seconds :   0

port 1/14 ETHERNET RECEIVE Performance Counters :
Frames :                2835    Bytes :                 3385891280
Pause Frames :          24      Broadcast Frames :      0
Dropped Frames :        0       Alignment Errors :      0
Oversize :              0       Undersize :             0
CRC Errors :            0       Carrier Sense Err :     0


port 1/14 ETHERNET TRANSMIT Performance Counters :
Frames :                3048    Bytes :                 3385891280
Pause Frames :          0

port 1/14 H.D.L.C Performance Counters :
CRC Errors :            3385891280      Invalid Frames :        0
Dropped Frames :        0

Console#
```

Table 29-13 show lre phys-info - display description

Field	Description
Performance Counters at Specified Interval	
Loss of frame	Number of seconds during which there was loss of framing
Loss of signal	Number of seconds during which there was loss of signal

Downloaded from www.Manualslib.com manuals search engine

Table 29-13 show lre phys-info - display description (Continued)

Field	Description
Loss of power	Number of seconds during which there was loss of power
Errored seconds	Number of seconds during which there was one or more CRC anomalies, or one or more Loss of Signal (LOS) or Loss of Framing (LOF) defects
Severely errored seconds	Number of seconds containing 18 or more CRC-8 anomalies, one or more Loss of Signal (LOS) defects, one or more Severely Errored Frame (SEF) defects, or one or more Loss of Power (LPR) defects.
Unavaliable seconds	Number of seconds during which the VDSL transceiver is powered up but not available
Ethernet Receive Performance Counters	
Frames	Number of frames (bad, broadcast and multicast) received.
Bytes	Number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Pause Frames	Number of MAC Control frames received with an opcode indicating the PAUSE operation.
Broadcast Frames	Number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Dropped Frames	Number of events in which frames were dropped due to lack of resources.
Alignment Errors	Number of alignment errors (missynchronized data packets).
Oversize	Number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Undersize	Number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
CRC Errors	Number of CRC errors (FCS or alignment errors).
Carrier Sense Errors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.

Downloaded from www.Manualslib.com manuals search engine

Table 29-13 show lre phys-info - display description (Continued)

Field	Description
Ethernet Transmit Performance Counters	
Frames	Number of frames (unicast, broadcast and multicast) transmitted.
Bytes	Number of bytes of data transmitted onto the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Pause Frames	Number of MAC Control frames transmitted with an opcode indicating the PAUSE operation.
High-Level Data-Link Control (H.D.L.C.) Performance Counters	
CRC Errors	Number of CRC errors (FCS or alignment errors).
Invalid Frames	Number of frames not properly bounded by flags, not containing an integral number of octets prior to zero-bit insertion or following zero-bit extraction, containing an FCS error, or containing an incorrect address field.
Dropped Frames	Number of frames dropped due to lack of resources.

Downloaded from www.Manualslib.com manuals search engine

CPE Configuration

This section describes operation and maintenance (OAM) functions for remote customer premises equipment (CPE), including upgrading firmware.

Table 29-14 CPE Configuration Commands

Command	Function	Mode	Page
Local Configuration			
oam local clear counter	Clears statistical data (in VDSL chip) for a specified VDSL port	IC	29-86
Remote Firmware Upgrade			
efm remote eeprom-write	Enables firmware upgrade on the CPE	IC	29-87
copy tftp firmware	Copies BME firmware used for upgrading CPEs from a TFTP server to reserved buffer space in the switch	GC	29-87
oam remote upgrade firmware	Copies BME firmware to the CPE	IC	29-90
oam remote firmware active	Activates alternate BME firmware version on CPE	IC	29-90
Displaying Remote OAM Information			
show cpe-info	Displays system information for a CPE connected to a VDSL port	PE	29-91

oam local clear counter

This command clears statistical data (in VDSL chip) for a specified VDSL port.

Command Mode

Interface Configuration

Command Usage

For information on the type of statistics maintained by the VDSL chip, see the **show lre perf** command on page 29-82.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#oam local clear counter
port 1 :        success to clear perfermance counters!
Console(config-if)#
```

efm remote eeprom-write

This command enables firmware upgrade on the CPE.

Syntax

efm remote eeprom-write {**enable** | **disable**}

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm remote eeprom-write enable
Console(config-if)#
```

copy tftp firmware

This command copies BME firmware used for upgrading CPEs from a TFTP server to reserved buffer space in the switch.

Command Mode

Global Configuration

Command Usage

- BME indicates the Burst Mode Engine used for digital signal processing.
- After using the **copy tftp firmware** command to copy BME firmware for CPEs to reserved buffer space in the switch, use the **oam remote upgrade firmware** command (page 29-90) to transfer the firmware to a remote CPE, and then use the oam remote firmware active command (page 29-90) to activate the new firmware.

Downloaded from www.Manualslib.com manuals search engine

Example

This example shows how to copy BME firmware for CPEs to a reserved buffer on the switch, copy this firmware to a remote CPE, and then activate the new firmware.

```
Console#show cpe-info 1/16
Protocol ID:                    Ikanos EOC Protocol
Protocol Version - Major:       01
Protocol Version - Minor:       01
Vendor ID (Value):              ffffffff (HEX), -1 (DECIMAL)
Host Application Version:       7.2.5r7IK104012
BME Firmware Version:           Firmware-VTU-R:7.2.5r7 Time May 19
2006,
                                RTOS Nucleus
AFE Hardware Version:           AFE<num: ver> <--:-->
IFE Hardware Version:           IFE<num:Dev.Rev> <0:a10>

Firmware Number:                2
Active Version:                 2
verId 1:                        NULL

verId 2:                        104012IK7.2.5r7

CO Firmware Buffer is empty now <------------
Console#copy tftp firmware
TFTP server IP address: 192.168.1.19
Source file name: 724maccpe
Success.
Firmware size :         485719
Firmware version :      104012IK7.2.4r9_Back_to_Back_Mac
Console#show cpe-info 1/16
Protocol ID:                    Ikanos EOC Protocol
Protocol Version - Major:       01
Protocol Version - Minor:       01
Vendor ID (Value):              ffffffff (HEX), -1 (DECIMAL)
Host Application Version:       7.2.5r7IK104012
BME Firmware Version:           Firmware-VTU-R:7.2.5r7 Time May 19
2006,
                                RTOS Nucleus
AFE Hardware Version:           AFE<num: ver> <--:-->
IFE Hardware Version:           IFE<num:Dev.Rev> <0:a10>

Firmware Number:                2
Active Version:                 2
verId 1:                        NULL

verId 2:                        104012IK7.2.5r7

CO Firmware Buffer version :    104012IK7.2.4r9_Back_to_Back_Mac
<-------
CO Firmware Buffer size :       485719
<-------
```


Downloaded from www.Manualslib.com manuals search engine

```
Console#configure
Console(config)#interface ethernet 1/16
Console(config-if)#oam remote upgrade firmware
Console(config)#end
Console#show cpe-info 1/16
Protocol ID:                    Ikanos EOC Protocol
Protocol Version - Major:       01
Protocol Version - Minor:       01
Vendor ID (Value):              ffffffff (HEX), -1 (DECIMAL)
Host Application Version:       7.2.5r7IK104012
BME Firmware Version:           Firmware-VTU-R:7.2.5r7 Time May 19
2006,
                                RTOS Nucleus
AFE Hardware Version:           AFE<num: ver> <--:-->
IFE Hardware Version:           IFE<num:Dev.Rev> <0:a10>

Firmware Number:                2
Active Version:                 2
verId 1:                        104012IK7.2.4r9_Back_to_Back_Mac
<-------

verId 2:                        104012IK7.2.5r7

CO Firmware Buffer version :    104012IK7.2.4r9_Back_to_Back_Mac
CO Firmware Buffer size :       485719
Console#configure
Console(config)#interface ethernet 1/16
Console(config-if)#oam remote firmware active
port 1/16:      Success to active remote firmware
Console(config)#end

Console#show cpe-info 1/16
Protocol ID:                    Ikanos EOC Protocol
Protocol Version - Major:       01
Protocol Version - Minor:       01
Vendor ID (Value):              ffffffff (HEX), -1 (DECIMAL)
Host Application Version:       7.2.5r7IK104012
BME Firmware Version:           Firmware-VTU-R:7.2.5r7 Time May 19
2006, RTOS Nucleus
AFE Hardware Version:           AFE<num: ver> <--:-->
IFE Hardware Version:           IFE<num:Dev.Rev> <0:a10>

Firmware Number:                2
Active Version:                 1
<-------
verId 1:                        104012IK7.2.4r9_Back_to_Back_Mac

verId 2:                        104012IK7.2.5r7

CO Firmware Buffer version :    104012IK7.2.4r9_Back_to_Back_Mac
CO Firmware Buffer size :       485719
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

oam remote upgrade firmware (page 29-90)
oam remote firmware active (page 29-90)

oam remote upgrade firmware

This command copies BME firmware to the CPE.

Command Mode

Interface Configuration

Command Usage

- BME indicates the Burst Mode Engine used for digital signal processing.
- Two firmware files can be stored on a CPE. The **oam remote firmware upgrade** command copies firmware to buffer space for the inactive version.
- After using the **copy tftp firmware** command (page 29-87) to copy BME firmware for CPEs to reserved buffer space in the switch, use the **oam remote upgrade firmware** command to transfer the firmware to a remote CPE, and then use the **oam remote firmware active** command (page 29-90) to activate the new firmware.

Example

Refer to the example under **copy tftp firmware** (page 29-87).

Related Commands

copy tftp firmware (page 29-87)
oam remote firmware active (page 29-90)

oam remote firmware active

This command activates the alternate (inactive) BME firmware version on the CPE.

Command Mode

Interface Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- BME indicates the Burst Mode Engine used for digital signal processing.
- This command activates the firmware version currently in inactive state. It can therefore be used to activate the firmware version copied to the CPE by the **oam remote upgrade firmware** command (page 29-90).
- After using the **copy tftp firmware** command (page 29-87) to copy BME firmware for CPEs to reserved buffer space in the switch, use the **oam remote upgrade firmware** command (page 29-90) to transfer the firmware to a remote CPE, and then use the **oam remote firmware active** command (page 29-90) to activate the new firmware.

Example

Refer to the example under **copy tftp firmware** (page 29-87).

Related Commands

copy tftp firmware (page 29-87)
oam remote upgrade firmware (page 29-90)

show cpe-info

This command displays system information for a CPE connected to a VDSL port.

Syntax

show cpe-info *unit/port*

- *unit* - Stack unit. (Range: 1)
- *port* - Port number. (Range: 1-16)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show cpe-info 1/1
Protocol ID:    Ikanos EOC Protocol
Protocol Version - Major:       01
Protocol Version - Minor:       01
Vendor ID (Value):      ffffffff (HEX), -1 (DECIMAL)
Host Application Version:     7.2.5r7IK104012
BME Firmware Version:           Firmware-VTU-R:7.2.5r7 Time May 19 2006,
RTOS Nucleus
AFE Hardware Version:         AFE<num: ver> <--:-->
IFE Hardware Version:         IFE<num:Dev.Rev> <0:a10>

Firmware Number:                2
Active Version:                 2
verId 1:                        NULL
verId 2:                        104012IK7.2.5r9

CO Firmware Buffer is empty now
Console#
```

Table 29-15 show cpe-info - display description

Field	Description
Protocol	Manufacturer ID, version numbers, and vendor ID
Host Application Version	Primary application firmware version
BME Firmware Version	Burst Mode Engine (DSP) firmware version
AFE Hardware Version	Analog Front End (DA/AD converter) hardware version
IFE Hardware Version	Integrated Front End (Port VDSL filtering) hardware version
Firmware Number	The number of firmware versions stored in this device.
Active Version	The firmware version currently in used by this device.
verId	The identifiers for the stored firmware versions.
CO Firmware Buffer	Status of the firmware download buffer.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 30
ADDRESS TABLE COMMANDS

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 30-1 Address Table Commands

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	30-2
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	30-3
show mac-address-table	Displays entries in the bridge-forwarding database	PE	30-4
mac-address-table aging-time	Sets the aging time of the address table	GC	30-5
show mac-address-table aging-time	Shows the aging time for the address table	PE	30-6

Downloaded from www.Manualslib.com manuals search engine

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface*
vlan *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)
  - **port-channel** *channel-id* (Range: 1-12)
- *vlan-id* - VLAN ID (Range: 1-4093)
- *action* -
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Downloaded from www.Manualslib.com manuals search engine

- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
  interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]]
[**interface** *interface*] [**vlan** *vlan-id*]
[**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)
  - **port-channel** *channel-id* (Range: 1-12)
- *vlan-id* - VLAN ID (Range: 1-4093)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."

Downloaded from www.Manualslib.com manuals search engine

- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 31
SPANNING TREE COMMANDS

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 31-1 Spanning Tree Commands

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	31-3
spanning-tree mode	Configures STP, RSTP or MSTP mode	GC	31-4
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	31-5
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	31-6
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	31-7
spanning-tree priority	Configures the spanning tree bridge priority	GC	31-8
spanning-tree path-cost method	Configures the path cost method for RSTP/MSTP	GC	31-9
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC	31-10
spanning-tree mst-configuration	Changes to MSTP configuration mode	GC	31-10
mst vlan	Adds VLANs to a spanning tree instance	MST	31-11
mst priority	Configures the priority of a spanning tree instance	MST	31-12
name	Configures the name for the multiple spanning tree	MST	31-13

Downloaded from www.Manualslib.com manuals search engine

Table 31-1 Spanning Tree Commands (Continued)

Command	Function	Mode	Page
revision	Configures the revision number for the multiple spanning tree	MST	31-14
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST	31-14
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC	31-15
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	31-16
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	31-18
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	31-18
spanning-tree portfast	Sets an interface to fast forwarding	IC	31-19
spanning-tree link-type	Configures the link type for RSTP/ MSTP	IC	31-21
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC	31-22
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC	31-23
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	31-24
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE	31-25
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE	31-27

Downloaded from www.Manualslib.com manuals search engine

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **spanning-tree**

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp** | **mstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)
- **mstp** - Multiple Spanning Tree (IEEE 802.1s)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP

Downloaded from www.Manualslib.com manuals search engine

restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol
  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

spanning-tree forward-time (31-5)
spanning-tree max-age (31-7)

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

spanning-tree forward-time (31-5)
spanning-tree hello-time (31-6)

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.
- **short** - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 31-16) takes precedence over port priority (page 31-18).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree mst-configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Setting

- No VLANs are mapped to any MST instance.
- The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

mst vlan (31-11)
mst priority (31-12)
name (31-13)
revision (31-14)
max-hops (31-14)

mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

[**no**] **mst** *instance_id* **vlan** *vlan-range*

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *vlan-range* - Range of VLANs. (Range: 1-4093)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 58 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 31-13) with the same set of instances, and the same

Downloaded from www.Manualslib.com manuals search engine

instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance_id* **priority** *priority*
no mst *instance_id* **priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *priority* - Priority of the a spanning tree instance.
  (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

name - Name of the spanning tree.

Default Setting

Switch's MAC address

Command Mode

MST Configuration

Command Usage

The MST region name and revision number (page 31-14) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

Related Commands

revision (31-14)

Downloaded from www.Manualslib.com manuals search engine

revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

Syntax

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

Default Setting

0

Command Mode

MST Configuration

Command Usage

The MST region name (page 31-13) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands

name (31-13)

max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

20

Command Mode

MST Configuration

Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

Syntax

[**no**] **spanning-tree spanning-disabled**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Downloaded from www.Manualslib.com manuals search engine

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the port.
(Range: 0 for auto-configuration, 1-65535 for short path cost method[34], 1-200,000,000 for long path cost method)

Table 31-2 Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 31-3 Recommended STA Path Cost

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

34. Use the spanning-tree pathcost method command on page 31-9 to set the path cost method.

Downloaded from www.Manualslib.com manuals search engine

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 31-4 Default STA Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 31-9) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost (31-16)

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

[**no**] **spanning-tree edge-port**

Downloaded from www.Manualslib.com manuals search engine

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (31-19)

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

[**no**] **spanning-tree portfast**

Default Setting

Disabled

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (31-18)

Downloaded from www.Manualslib.com manuals search engine

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```


Downloaded from www.Manualslib.com manuals search engine

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree mst *instance_id* **cost** *cost*
no spanning-tree mst *instance_id* **cost**

- *instance_id* - Instance identifier of the spanning tree.
  (Range: 0-4094, no leading zeroes)
- *cost* - Path cost for an interface.
  (Range: 0 for auto-configuration, 1-65535 for short path cost method[35], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 31-2 on page 31-16. The recommended path cost is listed in Table 31-3 on page 31-16.

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in Table 31-4 on page 31-17.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values

35. Use the spanning-tree pathcost method command on page 31-9 to set the path cost method.

Downloaded from www.Manualslib.com manuals search engine

should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.

- Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

spanning-tree mst port-priority (31-23)

spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance_id* **port-priority** *priority*
no spanning-tree mst *instance_id* **port-priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)
- *priority* - Priority for an interface. (Range: 0-240 in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

Downloaded from www.Manualslib.com manuals search engine

Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree mst cost (31-22)

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance_id*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)
  - **port-channel** *channel-id* (Range: 1-12)
- *instance_id* - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the **show spanning-tree mst** *instance_id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).
- For a description of the items displayed under "Spanning-tree information," see "Configuring Global Settings" on page 12-8. For a

Downloaded from www.Manualslib.com manuals search engine

description of the items displayed for specific interfaces, see "Displaying Interface Settings" on page 12-13.

Example

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode:                MSTP
 Spanning tree enable/disable:      enable
 Instance:                          0
 Vlans configuration:               1-4093
 Priority:                          32768
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Max hops:                          20
 Remaining hops:                    20
 Designated Root:                   32768.0.0000ABCD0000
 Current root port:                 1
 Current root cost:                 10000
 Number of topology changes:        1
 Last topology changes time (sec.): 22
 Transmission limit:                3
 Path Cost Method:                  long

---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status:             enable
 Role:                     root
 State:                    forwarding
 External admin path cost: 10000
 Internal admin cost:      10000
 External oper path cost:  10000
 Internal oper path cost:  10000
 Priority:                 128
 Designated cost:          200000
 Designated port:          128.24
 Designated root:          32768.0.0000ABCD0000
 Designated bridge:        32768.0.0030F1552000
 Fast forwarding:          disable
 Forward transitions:      1
 Admin edge port:          enable
 Oper edge port:           disable
 Admin Link type:          auto
 Oper Link type:           point-to-point
 Spanning Tree Status:     enable
:
```


Downloaded from www.Manualslib.com manuals search engine

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

Command Mode

Privileged Exec

Example

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-------------------------------------------------------------------
 Configuration name: R&D
 Revision level:0

 Instance Vlans
-------------------------------------------------------------------
     1    2
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 32
VLAN COMMANDS

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 32-1 VLAN Commands

Command Groups	Function	Page
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	32-2
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	32-7
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP	32-9
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	32-16
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	32-17
Configuring Protocol VLANs	Configures protocol-based VLANs based on frame type and protocol	32-20
Configuring 802.1Q Tunneling*	Configures IEEE 802.1Q tunneling (QinQ) to segregate and preserve customer VLAN IDs for traffic crossing the service provider network	32-25
Configuring VLAN Swapping*	Maps VLAN ID between customer and service provider for networks that do not support IEEE 802.1Q tunneling	32-30

* These functions are not compatible.

Downloaded from www.Manualslib.com manuals search engine

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 32-2 GVRP and Bridge Extension Commands

Command	Function	Mode	Page
bridge-ext gvrp	Enables GVRP globally for the switch	GC	32-2
show bridge-ext	Shows the global bridge extension configuration	PE	32-3
switchport gvrp	Enables GVRP for an interface	IC	32-4
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	32-15
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE	32-4
garp timer	Sets the GARP timer for the selected function	IC	32-5
show garp timer	Shows the GARP timer for the selected function	NE, PE	32-6

bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **bridge-ext gvrp**

Default Setting

Disabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Displaying Basic VLAN Information" on page 13-7 and "Displaying Bridge Extension Capabilities" on page 4-9 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support VLAN numbers:              256
 Max support VLAN ID:                   4093
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Disabled
 GMRP:                                  Disabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

Syntax

[**no**] **switchport gvrp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP configuration: Disabled
Console#
```


Downloaded from www.Manualslib.com manuals search engine

garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

join: 20 centiseconds
leave: 60 centiseconds
leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (32-6)

show garp timer

This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer:     20 centiseconds
 Leave timer:    60 centiseconds
 Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer (32-5)

Downloaded from www.Manualslib.com manuals search engine

Editing VLAN Groups

Table 32-3 Commands for Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	32-7
vlan	Configures a VLAN, including VID, name and state	VC	32-8

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (32-16)

Downloaded from www.Manualslib.com manuals search engine

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

show vlan (32-16)

Configuring VLAN Interfaces

Table 32-4 Commands for Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	32-9
switchport mode	Configures VLAN membership mode for an interface	IC	32-10
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	32-11
switchport ingress-filtering	Enables ingress filtering on an interface	IC	32-12
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	32-13
switchport allowed vlan	Configures the VLANs associated with an interface	IC	32-14
switchport gvrp	Enables GVRP for an interface	IC	32-4
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	32-15
switchport priority default	Sets a port priority for incoming untagged frames	IC	33-17

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (25-10)

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**hybrid | trunk | dot1q-tunnel**}
no switchport mode

- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.
- **dot1q-tunnel** - For an explanation of this command see page 32-27.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types (32-11)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

switchport mode (32-10)

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[**no**] **switchport ingress-filtering**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4093, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

All ports are assigned to VLAN 1 by default.

The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

Downloaded from www.Manualslib.com manuals search engine

- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

Displaying VLAN Information

This section describes commands used to display VLAN information.

Table 32-5 Commands for Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	32-16
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	25-13
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	25-16

show vlan

This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID:                1
Type:                   Static
Name:                   DefaultVlan
Status:                 Active
Ports/Port Channels:    Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                        Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                        Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                        Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S)
Console#
```

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This section describes commands used to configure private VlANs.

Table 32-6 Private VLAN Commands

Command	Function	Mode	Page
pvlan	Enables and configured private VLANS	GC	32-17
show pvlan	Displays the configured private VLANS	PE	32-19

pvlan

This command enables or configures a private VLAN. Use the **no** form to disable private VLANs, or the **no** form with the **group** keyword to disable a specific private VLAN group.

Syntax

pvlan [**up-link** *interface-list* **down-link** *interface-list* [**group** *group-number*]]
no pvlan [**group** *group-number*]

- **up-link** – Specifies an uplink interface including a port or trunk.
- **down-link** – Specifies a downlink interface including a port only.
- *group-number* – Number of independent private VLAN group. (Range: 1-5)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

No private VLANs are defined.
No default group exists.

Command Mode

Global Configuration

Command Usage

- A private VLAN provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port. Data cannot pass between downlink ports in the same private VLAN group, in other private VLAN groups, nor to ports which do not belong to a private VLAN.
- Up to five private VLAN groups can be defined. The same rules as stated above apply to each of the specified private VLAN groups.
- Any port can be defined as an uplink port or downlink port, but cannot configured to serve both roles. A downlink port can only be defined as a member of one private VLAN group, but an uplink port can be configured as a member of one or more private VLAN groups.
- Private VLANs and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in private VLANs and ports in normal VLANs.
- Enter the **pvlan** command without any parameters to enable the private VLAN functions. Then set the interface members for each private VLAN group.
- Enter **no pvlan** to disable private VLAN functions and clear the configuration settings for all groups, or for a specified group.

Example

This example enables the private VLAN, and then sets port 18 as the uplink and ports 5-8 as the downlinks.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/18 down-link ethernet
  1/1-5
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

show pvlan

This command displays the configured private VLAN.

Command Mode

Privileged Exec

Example

This example shows the information displayed when no group is defined.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/18 down-link ethernet 1/1-5
Console(config)#end
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/18
Down-link port:
 Ethernet 1/1
 Ethernet 1/2
 Ethernet 1/3
 Ethernet 1/4
 Ethernet 1/5
Console#
```

This example shows the information displayed a group is defined.

```
Console#show pvlan
Private VLAN status: Enabled
Group Uplink                          Downlink
----- ------------------------------- --------------------------------
  1   Eth1/18                         Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4
                                      Eth1/ 5
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 32-7 Protocol-based VLAN Commands

Command	Function	Mode	Page
protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC	32-21
protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC	32-22
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE	32-23
show interfaces protocol-vlan protocol-group	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE	32-24

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 32-8). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the **protocol-vlan protocol-group** command (General Configuration mode).

Downloaded from www.Manualslib.com manuals search engine

3. Then map the protocol for each interface to the appropriate VLAN using the **protocol-vlan protocol-group** command (Interface Configuration mode).

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{**add** | **remove**} **frame-type** *frame* **protocol-type** *protocol*]
no protocol-vlan protocol-group *group-id*

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *frame*[36] - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)
- *protocol* - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: ip, arp, rarp, pppoe8863 (PPPoE discover), pppoe8864 (PPPoE session), and user-defined (0801-FFFF hexadecimal).

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type
  ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type
  ethernet protocol-type arp
Console(config)#
```

36. SNAP frame types are not supported by this switch due to hardware limitations.

Downloaded from www.Manualslib.com manuals search engine

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*
no protocol-vlan protocol-group *group-id* **vlan**

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *vlan-id* - VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

Default Setting

No protocol groups are mapped for any interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as **vlan** on page 32-8), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Setting

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 ProtocolGroup ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                1      ethernet     08 00
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

   Port     ProtocolGroup ID    Vlan ID
---------- ------------------ -----------
   Eth 1/1                  1       vlan2
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Configuring IEEE 802.1Q Tunneling

QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 32-8 IEEE 802.1Q Tunneling Commands

Command	Function	Mode	Page
system mode	Configures the switch to operate in normal mode or QinQ mode	GC	20-13
show system mode	Displays the switch's system mode	GC	20-14
qinq priority map	Copies the priority bits from the inner VLAN tag to the outer VLAN tag	GC	32-26
switchport mode dot1q-tunnel	Configures an interface as a QinQ tunnel port	IC	32-27
show dot1q-tunnel	Displays information about QinQ tunnel ports	PE	32-28
switchport dot1q-ethertype	Sets the Tag Protocol Identifier (TPID) value of a tunnel port	IC	32-29

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (**system mode**, page 20-13).
2. Create a SPVLAN (**vlan**, page 32-8).
3. Configure the QinQ tunnel port to dot1Q tunnel port mode (**switchport mode dot1q-tunnel**, page 32-27).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See **switchport dot1q-ethertype**, page 32-29.)

Downloaded from www.Manualslib.com manuals search engine

5. Configure the QinQ tunnel port to join the SPVLAN as an untagged member (**switchport allowed vlan**, page 32-14).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel port (**switchport native vlan**, page 32-13).
7. Configure the QinQ uplink port to join the SPVLAN as a tagged member (**switchport allowed vlan**, page 32-14).

Limitations for QinQ

1. The native VLAN for the uplink ports and tunnel ports cannot be the same. However, the same service VLANs can be set on both uplink and tunnel ports.
2. IGMP Snooping should not be enabled on an access port.
3. If the spanning tree protocol is enabled, be aware that an access or tunnel port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

qinq priority map

This command copies the priority bits from the inner VLAN tag (used by the customer) to the outer VLAN tag (used by the service provider). Use the **no** form to disable this feature.

Syntax

[**no**] **qinq priority map**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Use the **switchport mode** command to set the switch to QinQ mode before entering this command.

Downloaded from www.Manualslib.com manuals search engine

- The packet must have a standard ethertype value of 0x8100 for this command to take effect. Otherwise, the priority bits in the outer tag are set to zero.
- Using a fixed priority level for all customer traffic allows the service provider to more easily calculate the resources required to maintain adequate bandwidth for a large number of customers. However, if it is necessary to support real-time services across the backbone network, then you may have to enable priority bit mapping from the inner to outer VLAN tag to ensure timely service.

Example

This example disables QinQ priority mapping, and uses the default port priority configured on the edge switch connecting the customer to the service provider's network.

```
Console(config)#no qinq priority map
Console(config)#
```

switchport mode dot1q-tunnel

This command configures an interface as a QinQ tunnel port. Use the **no** form to restore the default setting.

Syntax

switchport mode dot1q-tunnel
no switchport mode

dot1q-tunnel – Sets the port as an 802.1Q tunnel port.

Default Setting

All ports are in hybrid mode.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Use the **switchport mode** command to set the switch to QinQ mode before entering this command.
- When a tunnel port receives a packet from the customer, the customer tag (regardless of whether there are one or more tag layers) is copied

Downloaded from www.Manualslib.com manuals search engine

to the service provider's outer tag. The Tag Protocol Identifier (TPID) of the tunnel port is used for the outer tag. The default is for the standard ethertype value 0x8100, but may be changed to a non-standard value using the **switchport dot1q-ethertype** command (page 32-29). The tunnel port's native VLAN is used to process inbound packets. This can be modified using the **switchport native vlan**, command (page 32-13). And the priority bits set for the tunnel port are copied to the outer tag, unless this feature has been overridden by the **qinq priority map** command (page 32-26).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode dot1q-tunnel
Console(config-if)#
```

Related Commands

show dot1q-tunnel (page 32-28)
show interfaces switchport (page 25-16)

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

Command Mode

Privileged Exec

Example

```
Console(config)#system mode qinq
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode dot1q-tunnel
Console(config-if)#end
Console#show dot1q-tunnel
system mode is qinq
dot1q tunnel port:
ethernet 1/17
Console#
```

Related Commands

switchport mode dot1q-tunnel (page 32-27)

Downloaded from www.Manualslib.com manuals search engine

switchport dot1q-ethertype

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

Syntax

switchport dot1q-ethertype *tpid*
no switchport dot1q-ethertype

tpid – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0-ffff hexadecimal)

Default Setting

No dot1q-ethertype is set.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Use the **switchport dot1q-ethertype** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a tunnel port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port. The ethertype and priority bits of the tunnel port are also used to process the packet.
- All members of a VLAN should be set to the same ethertype.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-ethertype 9100
Console(config-if)#
```

Related Commands

show interfaces switchport (page 25-16)

Configuring VLAN Swapping

QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the local switches connected directly to the customer can be manually configured to swap the customer's VLAN ID with the service provider's VLAN ID.

This section describes commands used to configure VLAN swapping.

Table 32-9 VLAN Swapping Commands

Command	Function	Mode	Page
system mode	Enables VLAN ID swapping	GC	20-13
switchport vlan swap	Maps VLAN IDs between uplink and downlink ports	IC	32-31
show vlan swap	Displays VLAN swap configuration settings	PE	32-32
show system mode	Displays the switch's system mode	PE	20-14
show running-config	Displays the configuration data currently in use	PE	20-6

General Configuration Guidelines for VLAN Swapping

1. Configure the switch to VLAN Swap mode (**system mode**, page 20-13).
2. Enter Interface Configuration mode for the downlink port, and map the customer VLAN ID to the service provider's VLAN ID (**switchport vlan swap**, page 32-31) for traffic forwarded to the

Downloaded from www.Manualslib.com manuals search engine

uplink port (using the command parameters – input VLAN ID, output VLAN ID, and uplink interface).

3. Enter Interface Configuration mode for the uplink port, and map the service provider's VLAN ID to the customer's VLAN ID for traffic forwarded to the downlink port (using the command parameters – input VLAN ID, output VLAN ID, and downlink interface).

switchport vlan swap

This command maps VLAN IDs between uplink and downlink ports.

Syntax

switchport vlan swap *vlan-id1 vlan-id2 interface*
no switchport vlan swap {**all** | *vlan-id1 vlan-id2 interface*}

- *vlan-id1* - The VLAN ID to be replaced on traffic leaving the interface specified by the **interface** command. (Range: 1-4093)
- *vlan-id2* - The new VLAN ID to use on traffic entering the interface specified by the *interface* parameter in this command. (Range: 1-4093)
- **all** - Deletes all VLAN map entries for the current interface.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-18)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Use the **system mode vlan-swap** command (page 20-13) to enable VLAN swap mode globally on the switch, then use the switchport vlan swap command to map the customer VLAN ID to the service provider's VLAN ID.

Downloaded from www.Manualslib.com manuals search engine

- VLAN swapping only supports one-to-one mapping of VLAN IDs between a VDSL port and an uplink port.
- VLAN IDs must be mapped for both the upstream and downstream direction.
- The maximum number of VLAN swap entries is 64 per port groups 1-8, 9-16, 17, and 18. However, note that configuring a large number of entries may degrade the performance of other processes that also use the Fast Forwarding Processor (FFP) table, such as access lists, rate limiting, and IP filtering.

Example

This example configures VLAN swapping for upstream traffic between port 1 and port 18, exchanging VLAN ID 1 for VLAN ID 100. It then sets VLAN swapping for downstream traffic to exchange VLAN ID 100 for VLAN ID 1.

```
Console(config)#system mode vlan-swap
Console(config)#interface ethernet 1/1
Console(config-if)#switchport vlan swap 1 100 1/18
Console(config-if)#exit
Console(config)#interface ethernet 1/18
Console(config-if)#switchport vlan swap 100 1 1/1
Console(config-if)#
```

show vlan-swap

This command displays the VLAN swapping configuration settings.

Syntax

show vlan-swap [**interface** *interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-18)

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show vlan swap
vlan-swap enable
ethernet 1/1
    invlan    outvlan    outport
    1         100        1/18
ethernet 1/18
    invlan    outvlan    outport
    100       1          1/1
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 33
CLASS OF SERVICE COMMANDS

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Table 33-1 Priority Commands

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	33-1
Priority (Layer 3 and 4)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values	33-11

Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 33-2 Priority Commands (Layer 2)

Command	Function	Mode	Page
Global Priority Settings			
priority bits	Sets priority bits in the VLAN tag of packets sent by the CPU	GC	33-2
queue mode	Sets the queue mode to strict priority, Weighted Round-Robin (WRR), or hybrid	GC	33-3

Downloaded from www.Manualslib.com manuals search engine

Table 33-2 Priority Commands (Layer 2)

Command	Function	Mode	Page
show priority	Shows the priority bits used in packets sent by the CPU, and the IPv6 Traffic Class to Class-of-Service priority map	PE	33-4
show queue mode	Shows the current queue mode	PE	33-5
Port-based Priority Settings			
switchport priority default	Sets a port priority for incoming untagged frames	IC	33-17
queue bandwidth	Assigns round-robin weights to the priority queues	IC	33-7
queue cos-map	Assigns class-of-service values to the priority queues	IC	33-8
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	33-9
show queue cos-map	Shows the class-of-service map	PE	33-10
show interfaces switchport	Displays the administrative and operational status of an interface	PE	25-16

priority bits

This command sets the priority bits in the VLAN tag of packets sent by the CPU. Use the **no** form to restore the default value.

Syntax

[**no**] **priority bits**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

When priority bits are used in packets sent from the CPU, they are always set to CoS value 0. See Table 33-3, "Default CoS Priority

Downloaded from www.Manualslib.com manuals search engine

Levels," on page 33-8 for information on how CoS values are mapped to the output queues.

Example

```
Console(config)#priority bits
Console(config)#
```

queue mode

This command sets the queue mode to strict priority, Weighted Round-Robin (WRR), or a combination of both for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr** | **hybrid**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 - 7 respectively.
- **hybrid** - Strict priority is used for the high-priority queues and Weighted Round-Robin for the rest of the queues. The high priority queues are specified by setting a queue's bandwidth to zero with the **queue bandwidth** command (page 33-7).

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

- The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queueing.
- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.

Downloaded from www.Manualslib.com manuals search engine

- Weighted Round-Robin (WRR) specifies a relative weight of each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.
- Hybrid mode uses strict priority on the high-priority queues and WRR on the rest of the queues.
- Use the **queue bandwidth** command to assigns weights for WRR or hybrid mode to each of the priority queues. When using hybrid mode, set the queue bandwidth to zero to indicate the high-priority queues.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

Related Commands

queue bandwidth (33-7)
show queue mode (33-5)

show priority

This command shows the priority bits used in packets sent by the CPU, and the IPv6 Traffic Class to Class-of-Service priority map.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show priority
CPU TX Priority 0
PORT   Traffic-Class        Priority
1      1                    0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

priority bits (33-2)
priority ipv6 (33-17)

show queue mode

This command shows the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue mode

Wrr status: Enabled
Console#
```

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides eight priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

Related Commands

show interfaces switchport (25-16)

Downloaded from www.Manualslib.com manuals search engine

queue bandwidth

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues, or specifies a high-priority queue when the queue mode is set to hybrid. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight8*
no queue bandwidth

weight1...weight7 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 0 - 15)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- WRR controls bandwidth sharing at the egress port by defining scheduling weights for allocated service priorities.
- Use queue weights 1-15 for queues allocated service time based on WRR. Queue weights must be configured in ascendant manner, assigning more weight to each higher numbered queue.
- Use queue weight zero for high-priority queues processed with strict priority under the hybrid mode (see the **queue mode** command on page 33-3). Set queue bandwidth to zero to indicate a high-priority queue. Any of queues 2 - 7 can be specified as high-priority queues, but the selected queues must be in consecutive order, and must all be grouped toward the high end of the queue list as shown in the following example.

Downloaded from www.Manualslib.com manuals search engine

Example

This example assign WRR weights to priority queues 0-5, and strict priority to queues 6 and 7:

```
Console#configure
Console(config)#interface ethernet 1/5
Console(config-if)#queue bandwidth 1 3 5 7 9 11 0 0
Console(config-if)#
```

Related Commands

queue mode (33-3)
show queue bandwidth (33-9)

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.
  Ranges are 0 to 7, where 7 is the highest priority queue.
- *cos1 ... cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Table 33-3 Default CoS Priority Levels

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

CoS values assigned at the ingress port are also used at the egress port. This command sets the CoS priority for all interfaces.

Example

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

Related Commands

show queue cos-map (33-10)

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Default Setting

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0         1
    1         2
    2         4
    3         6
    4         8
    5         10
    6         12
    7         14
⋮
```

show queue cos-map

This command shows the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and Layer 4 traffic priority on the switch.

Table 33-4 Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip port	Enables TCP/UDP class of service mapping	GC	33-12
map ip port	Maps TCP/UDP socket to a class of service	IC	33-12
map ip precedence	Enables IP precedence class of service mapping	GC	33-13
map ip precedence	Maps IP precedence value to a class of service	IC	33-14
map ip dscp	Enables IP DSCP class of service mapping	GC	33-15
map ip dscp	Maps IP DSCP value to a class of service	IC	33-16
priority ipv6	Maps IPv6 traffic classes to priority queues for specified port	GC	33-17
show map ip port	Shows the IP port map	PE	33-17
show map ip precedence	Shows the IP precedence map	PE	33-19
show map ip dscp	Shows the IP DSCP map	PE	33-20
show priority	Shows the priority bits used in packets sent by the CPU, and the IPv6 Traffic Class to Class-of-Service priority map	PE	33-4

Downloaded from www.Manualslib.com manuals search engine

map ip port (Global Configuration)

This command enables IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

[**no**] **map ip port**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

This command sets IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- Up to 8 entries can be specified for IP Port priority mapping.
- This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Global Configuration)

This command enables IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

[**no**] **map ip precedence**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping.

Table 33-5 Mapping IP Precedence to CoS Values

IP Precedence Value	0	1	2	3	4	5	6	7
CoS Value	0	1	2	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP Precedence for all interfaces.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

[**no**] **map ip dscp**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - DSCP value. (Range: 0-63)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all of the DSCP values not specified are mapped to CoS value 0.

Table 33-6 Mapping IP DSCP to CoS Values

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

priority ipv6

This command assigns IPv6 traffic classes to one of the Class-of-Service values. Use the **no** form to restore the default setting.

Syntax

priority ipv6 *interface traffic-class cos-value*
no queue mode

- *interface*
  - *unit* - Stack unit. (Range: 1)
  - *port-list* - Single port number or list of ports. (Range: 1-18)
- *traffic-class* - IPv6 traffic class. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

No mapping is defined. All traffic classes are placed in the default priority queue – Queue 2 (the default queue for CoS 0).

Command Mode

Global Configuration

Command Usage

- The Traffic Class field in the IPv6 header may be used by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities for IPv6 packets. (See RFC 2460.)
- Nodes that support a specific use of some or all of the IPv6 traffic class bits are permitted to change the value of those bits in packets that they originate, forward, or receive, as required for that specific use. Nodes should ignore and leave unchanged any bits of the traffic class field for which they do not support a specific use.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example maps the Traffic Class value of 1 to CoS value 0:

```
Console(config)#priority ipv6 1 0
Console(config)#
```

show map ip port

This command shows the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Related Commands

map ip port (Global Configuration) (33-12)
map ip port (Interface Configuration) (33-12)

Downloaded from www.Manualslib.com manuals search engine

show map ip precedence

This command shows the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (33-13)
map ip precedence (Interface Configuration) (33-14)

Downloaded from www.Manualslib.com manuals search engine

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
⋮
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (33-15)
map ip dscp (Interface Configuration) (33-16)

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 34
QUALITY OF SERVICE COMMANDS

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 34-1 Quality of Service Commands

Command	Function	Mode	Page
class-map	Creates a class map for a type of traffic	GC	34-3
match	Defines the criteria used to classify traffic	CM	34-4
policy-map	Creates a policy map for multiple interfaces	GC	34-6
class	Defines a traffic classification for the policy to act on	PM	34-7
set	Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in a packet	PM-C	34-8
police	Defines an enforcer for classified traffic	PM-C	34-9
service-policy	Applies a policy map defined by the **policy-map** command to the input of a particular interface	IC	34-10
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE	34-11

Downloaded from www.Manualslib.com manuals search engine

Table 34-1 Quality of Service Commands (Continued)

Command	Function	Mode	Page
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE	34-12
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE	34-12

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the **class-map** command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the **match** command to select a specify type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Set an ACL mask to enable filtering for the criteria specified in the **match** command.
4. Use the **policy-map** command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
5. Use the **class** command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain multiple class statements.
6. Use the **set** command to modify the QoS value for matching traffic class, and use the **policer** command to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
7. Use the **service-policy** command to assign a policy map to a specific interface.

Downloaded from www.Manualslib.com manuals search engine

Notes: 1. You can configure up to 16 rules per Class Map. You can also include multiple classes in a Policy Map.
2. You should create a Class Map (page 34-3) before creating a Policy Map (page 34-6). Otherwise, you will not be able to specify a Class Map with the **class** command (page 34-7) after entering Policy-Map Configuration mode.

class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map and return to Global configuration mode.

Syntax

[**no**] **class-map** *class-map-name* [**match-any**]

- **match-any** - Match any condition within a class map.
- *class-map-name* - Name of the class map. (Range: 1-16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use the **match** command (page 34-4) to specify the criteria for ingress traffic that will be classified under this class map.
- Only one **match** command is permitted per class map, so the **match-any** field refers to the criteria specified by the lone **match** command for a class map.
- The class map uses the Access Control List filtering engine, so you must also set an ACL mask to enable filtering for the criteria specified in the **match** command. See "mask (IP ACL)" on page 24-9 or "mask (MAC ACL)" on page 24-21 for information on configuring an appropriate ACL mask.

Downloaded from www.Manualslib.com manuals search engine

- The class map is used with a policy map (page 34-6) to create a service policy (page 34-10) for a specific interface that defines packet classification, service tagging, and bandwidth policing.

Example

This example creates a class map call "rd_class," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

Related Commands

show class map (34-11)

match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

Syntax

[**no**] **match** {**access-list** *acl-name* | **ip dscp** *dscp* | **ip precedence** *ip-precedence* | **vlan** *vlan*}

- *acl-name* - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- *dscp* - A DSCP value. (Range: 0-63)
- *ip-precedence* - An IP Precedence value. (Range: 0-7)
- *vlan* - A VLAN. (Range:1-4094)

Default Setting

None

Command Mode

Class Map Configuration

Command Usage

- First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use the **match**

Downloaded from www.Manualslib.com manuals search engine

command to specify the fields within ingress packets that must match to qualify for this class map.

- Only one **match** command can be entered per class map.
- The class map uses the Access Control List filtering engine, so you must also set an ACL mask to enable filtering for the criteria specified in the **match** command. See "mask (IP ACL)" on page 24-9 and "mask (MAC ACL)" on page 24-21 for information on configuring an appropriate ACL mask.

Example

This example creates a class map called "rd_class#1," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

This example creates a class map call "rd_class#2," and sets it to match packets marked for IP Precedence service value 5:

```
Console(config)#class-map rd_class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call "rd_class#3," and sets it to match packets marked for VLAN 1:

```
Console(config)#class-map rd_class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```


Downloaded from www.Manualslib.com manuals search engine

policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map and return to Global configuration mode.

Syntax

[**no**] **policy-map** *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command (page 34-10).
- You must create a Class Map (page 34-6) before assigning it to a Policy Map.

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```


Downloaded from www.Manualslib.com manuals search engine

class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map and return to Policy Map configuration mode.

Syntax

[**no**] **class** *class-map-name*

class-map-name - Name of the class map. (Range: 1-16 characters)

Default Setting

None

Command Mode

Policy Map Configuration

Command Usage

- Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** and **police** commands to specify the match criteria, where the:
  - **set** command classifies the service that an IP packet will receive.
  - **police** command defines the maximum throughput, burst rate, and the action that results from a policy violation.
- You may only configure one rule per Class Map, but you can assign one or more classes to a policy map.

Downloaded from www.Manualslib.com manuals search engine

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

This command services IP traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified by the **match** command on page 34-4). Use the **no** form to remove the traffic classification.

Syntax

[**no**] **set** {**cos** *new-cos* | **ip dscp** *new-dscp* | **ip precedence** *new-precedence*}

- *new-cos* - New Class of Service (CoS) value. (Range: 0-7)
- *new-dscp* - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)
- *new-precedence* - New IP Precedence value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the

Downloaded from www.Manualslib.com manuals search engine

police command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

This command defines an policer for classified traffic. Use the **no** form to remove a policer.

Syntax

[**no**] **police** *rate-kbps burst-byte* [**exceed-action** {**drop** | **set**}]

- *rate-kbps* - Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
- *burst-byte* - Burst in bytes. (Range: 64-1522 bytes)
- **drop** - Drop packet when specified rate or burst are exceeded.
- **set** - Set DSCP service to the specified value. (Range: 0-63)

Default Setting

Drop out-of-profile packets.

Command Mode

Policy Map Class Configuration

Command Usage

- You can configure up to 63 policers (i.e., class maps) for Fast Ethernet and Gigabit Ethernet ingress ports.
- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *burst-byte* field, and the average rate tokens are removed from the bucket is by specified by the *rate-bps* option.

Downloaded from www.Manualslib.com manuals search engine

Example

This example creates a policy called "rd_policy," uses the **class** command to specify the previously defined "rd_class," uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

This command applies a policy map defined by the **policy-map** command to the ingress queue of a particular interface. Use the **no** form to remove the policy map from this interface.

Syntax

[**no**] **service-policy input** *policy-map-name*

- **input** - Apply to the input traffic.
- *policy-map-name* - Name of the policy map for this interface. (Range: 1-16 characters)

Default Setting

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can only assign one policy map to an interface.
- You must first define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.

Downloaded from www.Manualslib.com manuals search engine

Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-16 characters)

Default Setting

Displays all class maps.

Command Mode

Privileged Exec

Example

```
Console#show class-map
Class Map match-any rd_class#1
 Match ip dscp 3

Class Map match-any rd_class#2
 Match ip precedence 5

Class Map match-any rd_class#3
 Match vlan 1

Console#
```


Downloaded from www.Manualslib.com manuals search engine

show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

- *policy-map-name* - Name of the policy map. (Range: 1-16 characters)
- *class-map-name* - Name of the class map. (Range: 1-16 characters)

Default Setting

Displays all policy maps and all classes.

Command Mode

Privileged Exec

Example

```
Console#show policy-map
Policy Map rd_policy
 class rd_class
  set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
 class rd_class
  set ip dscp 3
Console#
```

show policy-map interface

This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface *interface* **input**

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Example

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 35
MULTICAST FILTERING COMMANDS

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 35-1 Multicast Filtering Commands

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	35-2
IGMP Query	Configures IGMP query parameters for multicast filtering	35-7
Static Multicast Routing	Configures static multicast router ports	35-12
IGMP Filtering and Throttling	Configures IGMP filtering and throttling	35-14
Multicast VLAN Registration	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic	35-23

Downloaded from www.Manualslib.com manuals search engine

IGMP Snooping Commands

This section describes commands used to configure IGMP snooping on the switch.

Table 35-2 IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	35-2
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	35-3
ip igmp snooping version	Configures the IGMP version for snooping	GC	35-4
ip igmp snooping immediate-leave	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	IC	35-5
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	35-6
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	35-6

ip igmp snooping

This command enables IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping**

Default Setting

Enabled

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)
  - **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
 ethernet 1/5
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2** | **3**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2
- **3** - IGMP Version 3

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. Note that the timeout period is determined by the **ip igmp snooping query-max-response-time** (see page 35-10).
- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp snooping immediate-leave
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

show ip igmp snooping

This command shows the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Configuring IGMP Snooping and Query Parameters" on page 16-4 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status:          Enabled
 Querier status:          Disabled
 Query count:             2
 Query interval:          125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version:   Version 2
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4093)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Downloaded from www.Manualslib.com manuals search engine

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

IGMP Query Commands

This section describes commands used to configure Layer 2 IGMP query on the switch.

Table 35-3 IGMP Query Commands

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	35-8
ip igmp snooping query-count	Configures the query count	GC	35-8
ip igmp snooping query-interval	Configures the query interval	GC	35-9
ip igmp snooping query-max-response-time	Configures the report delay	GC	35-10
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	35-11

Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping querier**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max- response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (35-10)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-25)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (35-4)
ip igmp snooping query-max-response-time (35-10)

Downloaded from www.Manualslib.com manuals search engine

ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (35-4)

Downloaded from www.Manualslib.com manuals search engine

Static Multicast Routing Commands

This section describes commands used to configure static multicast routing on the switch.

Table 35-4 Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	35-12
show ip igmp snooping mrouter	Shows multicast router ports	PE	35-13

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-19)
  - **port-channel** *channel-id* (Range: 1-12)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
Console#
```


Downloaded from www.Manualslib.com manuals search engine

IGMP Filtering and Throttling Commands

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 35-5 IGMP Filtering and Throttling Commands

Command	Function	Mode	Page
ip igmp filter	Enables IGMP filtering and throttling on the switch	GC	35-15
ip igmp profile	Sets a profile number and enters IGMP filter profile configuration mode	GC	35-16
permit, deny	Sets a profile access mode to permit or deny	IPC	35-16
range	Specifies one or a range of multicast addresses for a profile	IPC	35-17
ip igmp filter	Assigns an IGMP filter profile to an interface	IC	35-18
ip igmp max-groups	Specifies an IGMP throttling number for an interface	IC	35-18
ip igmp max-groups action	Sets the IGMP throttling action for an interface	IC	35-19
show ip igmp filter	Displays the IGMP filtering status	PE	35-20
show ip igmp profile	Displays IGMP profiles and settings	PE	35-21
show ip igmp throttle interface	Displays the IGMP throttling setting for interfaces	PE	35-22

Downloaded from www.Manualslib.com manuals search engine

ip igmp filter (Global Configuration)

This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

Syntax

[**no**] **ip igmp filter**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- IGMP filtering enables you to assign a profile to a switch port that specifies multcast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

Example

```
Console(config)#ip igmp filter
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

ip igmp profile

This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[**no**] **ip igmp profile** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny

This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

Syntax

{**permit** | **deny**}

Default Setting

Deny

Command Mode

IGMP Profile Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[**no**] **range** *low-ip-address* [*high-ip-address*]

- *low-ip-address* - A valid IP address of a multicast group or start of a group range.
- *high-ip-address* - A valid IP address for the end of a multicast group range.

Default Setting

None

Command Mode

IGMP Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
```


Downloaded from www.Manualslib.com manuals search engine

ip igmp filter (Interface Configuration)

This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

[**no**] **ip igmp filter** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- The IGMP filtering profile must first be created with the **ip igmp profile** command before being able to assign it to an interface.
- Only one profile can be assigned to an interface.
- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

Syntax

ip igmp max-groups *number*
no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 0-64)

Downloaded from www.Manualslib.com manuals search engine

Default Setting

64

Command Mode

Interface Configuration

Command Usage

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

This command sets the IGMP throttling action for an interface on the switch.

Syntax

ip igmp max-groups action {**replace** | **deny**}

- **replace** - The new multicast group replaces an existing group.
- **deny** - The new multicast group join report is dropped.

Default Setting

Deny

Command Mode

Interface Configuration

Downloaded from www.Manualslib.com manuals search engine

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

show ip igmp filter

This command displays the global and interface settings for IGMP filtering.

Syntax

show ip igmp filter [**interface** *interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show ip igmp filter
IGMP filter enable
Console#show ip igmp filter interface ethernet 1/1
Information of Eth 1/1
 IGMP Profile 19
  deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

This command displays IGMP filtering profiles created on the switch.

Syntax

show ip igmp profile [*profile-number*]

profile-number - An existing IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
  deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1)
  - *port* - Port number. (Range: 1-19)
- **port-channel** *channel-id* (Range: 1-12)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp throttle interface ethernet 1/1
Information of Eth 1/1
  status : TRUE
  action : deny
  max multicast groups : 32
  current multicast groups : 0
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Multicast VLAN Registration Commands

This section describes commands used to configure Multicast VLAN Registration (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 35-6 Multicast VLAN Registration Commands

Command	Function	Mode	Page
mvr	Globally enables MVR, statically configures MVR group address(es), or specifies the MVR VLAN identifier	GC	35-24
mvr	Configures an interface as an MVR receiver or source port, or configures an interface as a static member of the MVR VLAN	IC	35-26
mvr immediate	Enables immediate leave capability	IC	
show mvr	Shows information about the global MVR configuration settings, the interfaces attached to the MVR VLAN, or the multicast groups assigned to the MVR VLAN	PE	35-29

Downloaded from www.Manualslib.com manuals search engine

mvr (Global Configuration)

This command enables Multicast VLAN Registration (MVR) globally on the switch, enables a specific MVR domain using the **domain** keyword, statically configures MVR multicast group IP address(es) using the **group** keyword, or specifies the MVR VLAN identifier using the **vlan** keyword. Use the **no** form of this command without any keywords to globally disable MVR. Use the **no** form with the **domain** keyword to disable an MVR domain, the **group** keyword to remove a specific address or range of addresses, or the **vlan** keyword restore the default MVR VLAN.

Syntax

[**no**] **mvr**
[**domain** *domain-id* [**group** *ip-address* [*count*] |**vlan** *vlan-id*] |
group *ip-address* [*count*] | **vlan** *vlan-id*]

- *domain-id* - An independent multicast domain. (Range: 1-3)
- *ip-address* - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- *count* - The number of contiguous MVR group addresses. (Range: 1-255)
- *vlan-id* - MVR VLAN ID (Range: 1-4094)

Default Setting

- MVR is disabled.
- MVR domain ID is 1.
- No MVR group address is defined.
- The default number of contiguous addresses is 0.
- MVR VLAN ID is 1.

Command Mode

Global Configuration

Command Usage

- The following restrictions apply to the use of MVR domains:
  - MVR groups cannot overlap MVR domains.
  - The same VLAN cannot be assigned to different MVR domains.

Downloaded from www.Manualslib.com manuals search engine

- Use the **mvr group** command to statically configure all multicast group addresses that will join an MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

  The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see **ip igmp snooping** on page 35-2). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.
- IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

Example

The following example enables MVR globally, and configures a range of MVR group addresses:

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

mvr (Interface Configuration)

This command configures an interface as a static member of an MVR domain using the **group** keyword, or configures an interface as an MVR receiver or source port using the **type** keyword. Use the **no** form to restore the default settings.

Syntax

[**no**] **mvr**
{**domain** *domain-id* [**group** *ip-address* |**type** {**receiver** | **source**}] | **group** *ip-address* | **type** {**receiver** | **source**}}

- *domain-id* - An independent multicast domain. (Range: 1-3)
- *ip-address* - Statically configures an interface to receive multicast traffic from the IP address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- **receiver** - Configures the interface as a subscriber port that can receive multicast data.
- **source** - Configure the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

Default Setting

- MVR domain ID is 1.
- The port type is not defined.
- No port is a member of any configured multicast group.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- MVR source ports and receiver ports can be members of more than one MVR domain. However, an interface cannot be receiver port in one MVR domain and a source port in another domain.
- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- Receiver ports can belong to different VLANs. IGMP snooping can be used to allow a receiver port to dynamically join or leave multicast

Downloaded from www.Manualslib.com manuals search engine

groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port using the **group** keyword. However, if a receiver port is statically configured as a member of an MVR VLAN, its status will be inactive. Also, note that VLAN membership for MVR receiver ports cannot be set to trunk mode (see the **switchport mode** command on page 32-10).

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through IGMP snooping or which have been statically assigned using the **group** keyword.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see **ip igmp snooping** on page 35-2). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

Example

The following configures one source port and several receiver ports on the switch, enables immediate leave on one of the receiver ports, and statically assigns a multicast group to another receiver port:

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#mvr immediate
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr group 225.0.0.5
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

mvr immediate

This command causes the switch to immediately removes an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

Syntax

[**no**] **mvr immediate**

Default Setting

Disabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option only applies to an interface configured as an MVR receiver (see the **mvr** interface command on page 35-26).
- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
  - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
  - Immediate leave does not apply to multicast groups which have been statically assigned to a port.
  - The immediate leave command applies to all MVR domains.

Example

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate
Console(config-if)#
```


Downloaded from www.Manualslib.com manuals search engine

show mvr

This command shows information about the global MVR configuration settings when entered without any keywords, the interfaces attached to the MVR VLAN using the **interface** keyword, or the multicast groups assigned to the MVR VLAN using the **members** keyword.

Syntax

show mvr [**interface** [*interface*] | **members** [*ip-address*]]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1)
    - *port* - Port number. (Range: 1-18)
  - **port-channel** *channel-id* (Range: 1-12)
- *ip-address* - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Default Setting

Displays global configuration settings for MVR when no keywords are used.

Command Mode

Privileged Exec

Command Usage

Enter this command without any keywords to display the global settings for MVR. Use the **interface** keyword to display information about interfaces attached to the MVR VLAN. Or use the **members** keyword to display information about multicast groups assigned to the MVR VLAN.

Downloaded from www.Manualslib.com manuals search engine

Example

The following shows the global MVR settings:

```
Console#show mvr
================================
MVR domain : 1
MVR Status:enable
MVR running status:TRUE
MVR multicast vlan:1
MVR Max Multicast Groups:255
MVR Current multicast groups:1
================================
MVR domain : 2
MVR Status:disable
MVR running status:FALSE
MVR multicast vlan:0
MVR Max Multicast Groups:255
MVR Current multicast groups:0
================================
MVR domain : 3
MVR Status:disable
MVR running status:FALSE
MVR multicast vlan:0
MVR Max Multicast Groups:255
MVR Current multicast groups:0
Console#
```

Table 35-7 show mvr - display description

Field	Description
MVR Domain	An independent multicast domain.
MVR Status	Shows if MVR is globally enabled on the switch.
MVR running status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.)
MVR multicast vlan	Shows the VLAN used to transport all MVR multicast traffic.
MVR Max Multicast Groups	Shows the maximum number of multicast groups which can assigned to the MVR VLAN.
MVR Current multicast groups	Shows the number of multicast groups currently assigned to the MVR VLAN.

Downloaded from www.Manualslib.com manuals search engine

The following displays information about the interfaces attached to the MVR VLAN:

```
Console#show mvr interface
=====================================================
MVR domain : 1
Port    Type            Status          Immediate Leave
------- --------        -------------   ---------------
eth1/1  SOURCE          ACTIVE/UP         Disable
eth1/2  RECEIVER        ACTIVE/UP         Disable
eth1/5  RECEIVER        INACTIVE/DOWN     Disable
eth1/6  RECEIVER        INACTIVE/DOWN     Disable
eth1/7  RECEIVER        INACTIVE/DOWN     Disable
=====================================================
MVR domain : 2
Port    Type            Status          Immediate Leave
------- --------        -------------   ---------------
=====================================================
MVR domain : 3
Port    Type            Status          Immediate Leave
------- --------        -------------   ---------------
Console#
```

Table 35-8 show mvr interface - display description

Field	Description
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is "ACTIVE" if MVR is globally enabled on the switch. MVR status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
Immediate Leave	Shows if immediate leave is enabled or disabled.

Downloaded from www.Manualslib.com manuals search engine

The following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN:

```
Console#show mvr members
==================================
MVR domain : 1
MVR Group IP      Status    Members
---------------  --------  -------
225.0.0.1         ACTIVE    eth1/1(d), eth1/2(s)
225.0.0.2         INACTIVE  None
225.0.0.3         INACTIVE  None
225.0.0.4         INACTIVE  None
225.0.0.5         INACTIVE  None
225.0.0.6         INACTIVE  None
225.0.0.7         INACTIVE  None
225.0.0.8         INACTIVE  None
225.0.0.9         INACTIVE  None
225.0.0.10        INACTIVE  None
==================================
MVR domain : 2
MVR Group IP      Status    Members
---------------  --------  -------
==================================
MVR domain : 3
MVR Group IP      Status    Members
---------------  --------  -------
Console#
```

Table 35-9 show mvr members - display description

Field	Description
MVR Group IP	Multicast groups assigned to the MVR VLAN.
Status	Shows whether or not the there are active subscribers for this multicast group. Note that this field will also display "INACTIVE" if MVR is globally disabled.
Members	Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows if an interface has dynamically joined a multicast group (**d**), or if a multicast group has been statically bound to the interface (**s**).

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 36
DOMAIN NAME SERVICE COMMANDS

These commands are used to configure Domain Naming System (DNS) services. You can manually configure entries in the DNS domain name to IP address mapping table, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the **ip name-server** command and domain lookup is enabled with the **ip domain-lookup** command.

Table 36-1 DNS Commands

Command	Function	Mode	Page
ip host	Creates a static host name-to-address mapping	GC	36-2
clear host	Deletes entries from the host name-to-address table	PE	36-3
ip domain-name	Defines a default domain name for incomplete host names	GC	36-4
ip domain-list	Defines a list of default domain names for incomplete host names	GC	36-5
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC	36-6
ip domain-lookup	Enables DNS-based host name-to-address translation	GC	36-7
show hosts	Displays the static host name-to-address mapping table	PE	36-8
show dns	Displays the configuration for DNS services	PE	36-9

Downloaded from www.Manualslib.com manuals search engine

Table 36-1 DNS Commands (Continued)

Command	Function	Mode	Page
show dns cache	Displays entries in the DNS cache	PE	36-9
clear dns cache	Clears all entries from the DNS cache	PE	36-10

ip host

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the **no** form to remove an entry.

Syntax

[**no**] **ip host** *name address1* [*address2* … *address8*]

- *name* - Name of the host. (Range: 1-127 characters)
- *address1* - Corresponding IP address.
- *address2* … *address8* - Additional corresponding IP addresses.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.

Downloaded from www.Manualslib.com manuals search engine

Example

This example maps two address to a host name.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias

Console#
```

clear host

This command deletes entries from the DNS table.

Syntax

clear host {*name* | *}

- *name* - Name of the host. (Range: 1-127 characters)
- * - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Example

This example clears all static entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```


Downloaded from www.Manualslib.com manuals search engine

ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

Syntax

ip domain-name *name*
no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-63 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
Name Server List:
Console#
```

Related Commands

ip domain-list (36-5)
ip name-server (36-6)
ip domain-lookup (36-7)

Downloaded from www.Manualslib.com manuals search engine

ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

Syntax

[**no**] **ip domain-list** *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-63 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the **ip domain-name** command is used. If there is a domain list, the default domain name is not used.

Downloaded from www.Manualslib.com manuals search engine

Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
Console#
```

Related Commands

ip domain-name (36-4)

ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

[**no**] **ip name-server** *server-address1* [*server-address2* … *server-address6*]

- *server-address1* - IP address of domain-name server.
- *server-address2* … *server-address6* - IP address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Downloaded from www.Manualslib.com manuals search engine

Example

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name (36-4)
ip domain-lookup (36-7)

ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[**no**] **ip domain-lookup**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- At least one name server must be specified before you can enable DNS.
- If all name servers are deleted, DNS will automatically be disabled.

Downloaded from www.Manualslib.com manuals search engine

Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
```

Related Commands

ip domain-name (36-4)
ip name-server (36-6)

show hosts

This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```


Downloaded from www.Manualslib.com manuals search engine

show dns

This command displays the configuration of the DNS service.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
2         4     CNAME   66.218.71.84    298     www.yahoo.akadns.net
3         4     CNAME   66.218.71.83    298     www.yahoo.akadns.net
4         4     CNAME   66.218.71.81    298     www.yahoo.akadns.net
5         4     CNAME   66.218.71.80    298     www.yahoo.akadns.net
6         4     CNAME   66.218.71.89    298     www.yahoo.akadns.net
7         4     CNAME   66.218.71.86    298     www.yahoo.akadns.net
8         4     ALIAS   POINTER TO:7    298     www.yahoo.com
Console#
```


Downloaded from www.Manualslib.com manuals search engine

Table 36-2 show dns cache - display description

Field	Description
NO	The entry number for each resource record.
FLAG	The flag is always "4" indicating a cache entry and therefore unreliable.
TYPE	This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
IP	The IP address associated with this record.
TTL	The time to live reported by the name server.
DOMAIN	The domain name associated with this record.

clear dns cache

This command clears all entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#clear dns cache
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
Console#
```


Downloaded from www.Manualslib.com manuals search engine

CHAPTER 37
DHCP COMMANDS

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client and relay functions. You can configure any VLAN interface to be automatically assigned an IP address via DHCP. This switch can also be configured to relay DHCP client configuration requests to a DHCP server on another network.

Table 37-1 DHCP Commands

Command Group	Function	Page
DHCP Client	Allows interfaces to dynamically acquire IP address information	37-1
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server	37-2

DHCP Client

Table 37-2 DHCP Client Commands

Command	Function	Mode	Page
ip dhcp restart	Submits a BOOTP or DHCP client request	PE	37-1

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.1.54, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip address (38-2)

DHCP Relay

Table 37-3 DHCP Relay Commands

Command	Function	Mode	Page
ip dhcp relay server	Specifies DHCP server addresses for relay	GC	37-3
ip dhcp information option	Enables DHCP Option 82 information relay, and specifies the frame format	GC	37-4
ip dhcp information policy	Specifies how to handle DHCP client requests which already contain Option 82 information	GC	37-6
show ip dhcp relay server	Displays the configuration settings for DHCP relay service	PE	37-7

Downloaded from www.Manualslib.com manuals search engine

ip dhcp relay server

This command enables DHCP relay service, and specifies the address of the server to use. Use the **no** form to clear a server address.

Syntax

ip dhcp relay server *address*
no ip dhcp relay server

address - IP address of a DHCP server.

Default Setting

None

Command Mode

Global Configuration

Usage Guidelines

- DHCP relay service only applies to the management VLAN. DHCP client request packets entering any other VLAN on the switch will be flooded.
- This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled (by specifying the address for at least one DHCP server), and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.
- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server. Up to five DHCP servers can be specified.
- To terminate DHCP relay service, all configured server addresses must be cleared with the **no** form of this command.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console(config)#ip dhcp relay server 192.168.10.19
Console(config)#
```

ip dhcp information option

This command enables DHCP Option 82 information relay, and specifies the frame format to use when Option 82 information is generated by the switch. Use the **no** form of this command to disable this feature.

Syntax

ip dhcp information option {**circuit-id** | **remote-id**}
no ip dhcp information option

- **circuit-id** - Includes fields which identify the incoming circuit, including the VLAN, stack unit, and port.
- **remote-id** - Includes a MAC address field for the relay agent (that is, the MAC address of the switch's CPU).

Default Setting

Disabled

Command Mode

Global Configuration

Usage Guidelines

- DHCP provides a relay agent information option for sending information about its DHCP clients to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients.
- When Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. Depending on the selected option frame format, this information may specify the circuit which received the request (including VLAN, stack unit, and port), or just the MAC address of the requesting device.

Downloaded from www.Manualslib.com manuals search engine

- If Option 82 is enabled on the switch, client information will be included in any relayed request packet received through the management interface according to this criteria.

Table 37-4 Inserting Option 82 Information

DHCP Snooping*	DHCP Relay†	DHCP Option 82	Action
Enabled	Disabled	Enabled	Circuit-id or remote-id information is added to the Option 82 packet, but the gateway Internet address is not included.
Disabled	Enabled	Enabled	Circuit-id or remote-id information is added to the option 82 packet, and the gateway Internet address is included.
Enabled	Enabled	Enabled	Circuit-id or remote-id information is added to the option 82 packet, and the gateway Internet address is included.

* See **ip dhcp snooping** on page 23-18.
† See **ip dhcp relay server** on page 37-3.

- DHCP request packets are flooded onto all attached VLANs other than the inbound VLAN under the following situations:
  - Neither DHCP snooping nor DHCP relay are enabled.
  - The request packet contains a valid relay agent address field.
  - The request packet is received on a non-management VLAN.
- DHCP reply packets received by the relay agent are handled in the following manner:
  1. When the relay agent receives a DHCP reply packet with Option 82 information on the management VLAN, it first ensures that the packet is destined for it, and then removes the Option 82 field from the packet.
  2. If the DHCP packet's broadcast flag is on, the reply packet is broadcast to all attached VLANs, excluding that through which

Downloaded from www.Manualslib.com manuals search engine

the reply packet was received. If the DHCP packet's broadcast flag is off, the switch uses the Option 82 information to identify the interface connected to the requesting client and unicasts the reply packet to the client.

- DHCP reply packets are flooded onto all attached VLANs other than the inbound management VLAN under the following situations:
  - The reply packet does not contain Option 82 information.
  - The reply packet contains a valid relay agent address field (that is not the address of this switch) or a zero relay address.
- Use the **ip dhcp information policy** command (page 37-6) to specify how to handle DHCP client request packets which already contain Option 82 information.

Example

This example enables Option 82, and sets the frame format for the option to use a circuit identifier.

```
Console(config)#ip dhcp information option circuit-id
Console(config)#
```

Related Commands

ip dhcp information policy (37-6)
ip dhcp relay server (37-3)
ip dhcp snooping (23-18)

ip dhcp information policy

This command specifies how to handle client requests which already contain DHCP Option 82 information.

Syntax

ip dhcp information policy {**drop** | **keep** | **replace**}

- **drop** - Drop the request packet instead of relaying it.
- **keep** - Retain the Option 82 information in the client request, insert the relay agent's address (when DHCP snooping or relay is enabled), and unicast the packet to the DHCP server.
- **replace** - Replace the Option 82 information in the client's request with information about the relay agent itself, insert the relay agent's

Downloaded from www.Manualslib.com manuals search engine

address (when DHCP snooping or relay is enabled), and unicast the packet to the DHCP server.

Default Setting

replace

Command Mode

Global Configuration

Usage Guidelines

- Refer to the Usage Guidelines under the **ip dhcp information option** command (page 37-4) for information on when Option 82 information is processed by the switch.
- When the Option 82 policy is set to "keep" the original information in the request packet, the frame type specified by the **ip dhcp information option** command is ignored.

Example

This example sets the Option 82 policy to keep the client information in the request packet received by the relay agent, and forward this packet on to the DHCP server.

```
Console(config)#ip dhcp information policy keep
Console(config)#
```

Related Commands

ip dhcp information option (37-4)
ip dhcp relay server (37-3)
ip dhcp snooping (23-18)

show ip dhcp relay server

This command displays the configuration settings for DHCP relay service.

Command Mode

Privileged Exec

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#show ip dhcp relay server
  Ip Dhcp Relay Status: Enable
  Ip Dhcp Relay Server: 192.168.10.19
  DHCP Information Option Circuitid Status: disable
  DHCP Information Option Remoteid Status: disable
  DHCP Information Policy: replace
Console#
```

Related Commands

ip dhcp relay server (37-3)

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 38
IP INTERFACE COMMANDS

An IP address may be used for management access to the switch over your network. An IP address is obtained via DHCP by default for VLAN 1. You can manually configure a specific IP address, or direct the switch to obtain an address from a BOOTP or DHCP server when it is powered on. You may also need to a establish a default gateway between this device and management stations that exist on another network segment.

Basic IP Configuration

This section describes commands used to configure an IP address for the switch

Table 38-1 Basic IP Configuration Commands

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	38-2
ip default-gateway	Defines the default gateway through which this router can reach other subnetworks	GC	38-3
show ip interface	Displays the IP settings for this device	PE	38-4
show ip redirects	Displays the default gateway configured for this device	PE	38-4
ping	Sends ICMP echo request packets to another node on the network	NE, PE	38-5

Downloaded from www.Manualslib.com manuals search engine

ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

DHCP

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network or to connect the switch to existing IP subnets. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by rebooting the switch.

Downloaded from www.Manualslib.com manuals search engine

Notes: 1. Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

2. Before you can change the IP address, you must first clear the current address with the **no** form of this command.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

ip default-gateway

This command specifies the IP default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

- A gateway must be defined if the management station is located in a different IP segment.
- An default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects (38-4)

show ip interface

This command displays the settings of an IP interface.

Command Mode

Privileged Exec

Example

```
Console#show ip interface

Console#
```

Related Commands

show ip redirects (38-4)

show ip redirects

This command shows the IP default gateway configured for this device.

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (38-3)

Downloaded from www.Manualslib.com manuals search engine

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*][**size** *size*]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Downloaded from www.Manualslib.com manuals search engine

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (25-2)

Downloaded from www.Manualslib.com manuals search engine

SECTION IV
APPENDICES

This section provides additional information on the following topics.

Software Specifications A-1
Troubleshooting B-1
Glossary
Index

Downloaded from www.Manualslib.com manuals search engine

Appendices

Downloaded from www.Manualslib.com manuals search engine

APPENDIX A
SOFTWARE SPECIFICATIONS

Software Features

Authentication
Local, RADIUS, TACACS+, Port (802.1X), HTTPS, SSH, Port Security

Access Control Lists
IP, MAC
Fast Ethernet ports - 173 rules, 7 masks shared by 8-port groups
Gigabit Ethernet ports - 52 rules, 7 masks

DHCP Client, Relay

BOOTP Client

DNS Proxy

Port Configuration
VDSL2: 10/100 Mbps at half/full duplex (16 ports on RJ-21 connector)
100BASE-TX: 10/100 Mbps at half/full duplex (RJ-45 management port)
1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP)

Flow Control
Full Duplex: IEEE 802.3x
Half Duplex: Back pressure

Storm Control
Broadcast, multicast, unknown unicast traffic throttled above a critical threshold

Port Mirroring
Multiple source ports, one destination port

Downloaded from www.Manualslib.com manuals search engine

Rate Limits
Input/output limit
Range (configured per port)

Port Trunking
Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Algorithm
Spanning Tree Protocol (STP, IEEE 802.1D)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)
Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s)

VLAN Support
Up to 256 groups; port-based, protocol-based, or tagged (802.1Q), GVRP for automatic VLAN learning, QinQ double-tagging, private VLANs

Class of Service
Supports eight levels of priority and Weighted Round Robin Queueing (which can be configured by VLAN tag, IPv6 priority bits, or port), Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

Quality of Service
DiffServ supports class maps, policy maps, and service policies

Multicast Filtering
IGMP Snooping
Multicast VLAN Registration

VDSL2
Frequency division duplexing separates upstream and downstream transmissions
Up to 6 bands with spectrum utilization of up to 30MHz
Maximum symmetrical short range bit rate of 100 Mbps at 200 meters
Rate Adaptive mode automatically sets optimal rate for existing line conditions
RFI Notching per ITU-T and TTC requirements

Downloaded from www.Manualslib.com manuals search engine

3 OAM channels (IB, eoc, VOC) between VTU-C and VTU-R
HDLC or 802.3ah EFM framing
Upstream power back off
CPE firmware-upgrade via eoc channel
Remote CPE management, reset, auto-configuration and performance monitoring

Additional Features
BOOTP client
SNTP (Simple Network Time Protocol)
SNMP (Simple Network Management Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts

Management Features

In-Band Management
Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management
RS-232 DB-9 console port

Software Loading
TFTP in-band or XModem out-of-band

SNMP
Management access via MIB database
Trap management to specified hosts

RMON
Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags

Downloaded from www.Manualslib.com manuals search engine

IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1s Multiple Spanning Tree Protocol
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1X Port Authentication
IEEE 802.3-2002
  Ethernet, Fast Ethernet, Gigabit Ethernet
  Link Aggregation Control Protocol (LACP)
  Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
ITU-T G.993.1 (VDSL) and G.993.2 (VDSL2)
ITU-T G.994.1 (VDSL handshake compliance)
ARP (RFC 826)
DHCP Client (RFC 2131)
DHCP Relay (RFC 3046)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IPv4 IGMP (RFC 3228)
RADIUS+ (RFC 2618)
RMON (RFC 2819 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 2571)
SNMPv3 (RFC DRAFT 3414, 3410, 2273, 3411, 3415)
SNTP (RFC 2030)
SSH (Version 2.0)
TFTP (RFC 1350)

Management Information Bases

Bridge MIB (RFC 1493)
DNS Resolver MIB (RFC 1612)
Differentiated Services MIB (RFC 3289)

Downloaded from www.Manualslib.com manuals search engine

Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP MIB (RFC 2011)
IP Multicasting related MIBs
MAU MIB (RFC 3636)
MIB II (RFC 1213)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Private MIB
QnQ Tunneling (IEEE 802.1ad Provider Bridges)
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMPv2 IP MIB (RFC 2011)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMP Community MIB (RFC 3584)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

APPENDIX B
TROUBLESHOOTING

Problems Accessing the Management Interface

Table B-1 Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	• Be sure the switch is powered up. • Check network cabling between the management station and the switch. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.

Downloaded from www.Manualslib.com manuals search engine

Table B-1 Troubleshooting Chart (Continued)

Symptom	Action
Cannot connect using Secure Shell	• If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. • Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. • Be sure you have generated a public key on the switch, and exported this key to the SSH client. • Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. • Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact your local distributor.

Downloaded from www.Manualslib.com manuals search engine

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Designate the SNMP host that is to receive the error messages.
4. Repeat the sequence of commands or other actions that lead up to the error.
5. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
6. Contact your distributor's service engineer.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
⋮
```


Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

GLOSSARY

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services (DiffServ)

DiffServ provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be

Downloaded from www.Manualslib.com manuals search engine

marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Downloaded from www.Manualslib.com manuals search engine

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

Downloaded from www.Manualslib.com manuals search engine

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

Downloaded from www.Manualslib.com manuals search engine

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message-Digest Algorithm

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Downloaded from www.Manualslib.com manuals search engine

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1X.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Plain Old Telephone Service (POTS)

One of the services using voice band. Sometimes used as a descriptor for all voice band services.

Downloaded from www.Manualslib.com manuals search engine

Private Branch Exchange (PBX)

A telephone exchange local to a particular organization who use, rather than provide, telephone services.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Quality of Service (QoS)

QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Downloaded from www.Manualslib.com manuals search engine

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Algorithm (STA)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Splitter

A filter to separate VDSL signals from POTS or ISDN signals to prevent mutual interference.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Downloaded from www.Manualslib.com manuals search engine

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Universal Time Coordinate (UTC)

UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Very high data rate Digital Subscriber Line (VDSL)

A family of digital telecommunications protocols designed to allow high speed data communication at data rates from below 1 Mbps to 52.8 Mbps with corresponding maximum reach ranging from 4500 feet to 1000 feet using 24 gauge twisted pair cable over the existing copper telephone lines between end-users and service providers.

Downloaded from www.Manualslib.com manuals search engine

Very high data rate Digital Subscriber Line 2 (VDSL2)

VDSL2 as defined in ITU-T Recommendation G.993.2 is an enhancement to the first VDSL standard (G.993.1). It supports transmission at a bi-directional net data rate (the sum of upstream and downstream rates) of up to 200 Mbps on twisted pair cables using a bandwidth of up to 30 MHz. VDSL2 includes many enhancements, one of which is the addition of the US0 band and methods to train echo cancellers and time domain equalizers.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Downloaded from www.Manualslib.com manuals search engine

INDEX

Numerics

802.1Q tunnel 13-24, 32-25
  description 13-24
  interface configuration 13-30, 32-27—32-29
  mode selection 13-30, 32-10, 32-27
  TPID 13-30, 32-29
802.1X, port authentication 6-19, 22-34

A

acceptable frame type 13-15, 32-11
Access Control List *See* ACL
ACL
  Extended IP 8-2, 8-3, 8-5, 24-2, 24-5
  MAC 8-2, 8-3, 24-16
  Standard IP 8-2, 8-3, 8-4, 24-2, 24-4
address table 11-1, 30-1
  aging time 11-4, 30-6
alarm profile, VDSL 10-30, 29-51

B

BOOTP 4-14, 38-2
BPDU 12-2
broadcast storm, threshold 9-23, 25-11

C

Class of Service *See* CoS
CLI
  command modes 18-7
  main menu 18-12
  showing commands 18-5
client security 7-1, 23-1
command line interface *See* CLI
community string 2-11, 5-4, 21-4
configuration files, restoring defaults 4-20, 20-16
configuration settings, saving or restoring 2-15, 4-20, 20-16, 20-17
console port, required connections 2-2
CoS
  configuring 14-1, 33-1
  DSCP 14-13, 33-15
  IP port priority 14-16, 33-12
  IP precedence 14-11, 33-13
  IPv6 traffic classes 14-15, 33-17
  layer 3/4 priorities 14-9, 33-11
  queue mapping 14-3, 33-8
  queue mode 14-6, 33-3
  traffic class weights 14-7, 33-7
CPU
  status 4-4, 20-11
  utilization alarm 4-4

D

default IP gateway, configuration 4-12, 38-3
default priority, ingress port 14-1, 33-5
default settings, system 1-9
DHCP 4-14, 38-2
  client 4-11, 37-1
  dynamic configuration 2-9, 4-14, 38-2
  relay 37-2
  relay option 82 37-4
  snooping 7-8, 23-17
DHCP snooping
  converting dynamic to static address 7-11, 23-22
  global configuration 7-10, 23-18
  limiting number of clients attached to a port 7-11, 23-23
  specifying trusted interfaces 7-11, 23-24

Downloaded from www.Manualslib.com manuals search engine

verifying MAC addresses 7-10, 23-21
VLAN configuration 7-10, 23-20
Differentiated Code Point Service *See* DSCP
Differentiated Services *See* DiffServ
DiffServ 15-2, 34-1
binding policy to interface 15-10, 34-10
class map 15-3, 34-3, 34-7
policy map 15-6, 34-6
service policy 15-10, 34-10
DNS
default domain name 17-1, 36-4
displaying the cache 17-6, 36-9
domain name list 17-1, 36-2
enabling lookup 17-1, 36-7
name server list 17-1, 36-6
static entries 17-4, 36-2
Domain Name Service *See* DNS
downloading software 4-18, 20-17
DSCP
enabling 14-10, 33-15
mapping priorities 14-13, 33-16
dynamic addresses, displaying 11-2, 30-4
Dynamic Host Configuration Protocol *See* DHCP

E

edge port, STA 12-16, 12-20, 31-18
engine ID 5-10, 21-10
event logging 4-29, 20-39

F

fan status 4-4, 20-8
filtering
DHCP replies 7-15, 23-9
DHCP requests 7-15, 23-8
IP/MAC address pairs 7-18, 23-5
NetBIOS traffic 7-15, 23-7
firmware
displaying VDSL chip version 20-10
displaying version 4-7, 20-10
upgrading 4-18, 20-17

G

GARP VLAN Registration Protocol *See* GVRP
gateway, IP default 4-12, 38-3
GVRP
global setting 13-6, 32-2
interface configuration 13-16, 32-4

H

hardware status 4-4, 20-8
hardware version, displaying 4-7, 20-10
HTTPS 6-7, 22-17
secure-site certificate 6-9
HTTPS, secure server 6-7, 22-17

I

IEEE 802.1D 12-1, 31-4
IEEE 802.1s 12-1, 31-4
IEEE 802.1w 12-1, 31-4
IEEE 802.1X 6-19, 22-34
IGMP
filtering/throttling 16-14, 35-14
filtering/throttling, configuring profile 16-16, 35-16, 35-17
filtering/throttling, creating profile 16-15, 35-16
filtering/throttling, enabling 16-15, 35-15
filtering/throttling, interface settings 16-18, 35-18—35-19
groups, displaying 16-9, 35-6

Downloaded from www.Manualslib.com manuals search engine

Layer 2 16-2, 35-2
query 16-2, 35-8
query, Layer 2 16-4, 35-7
snooping 16-2, 35-2
snooping, configuring 16-4, 35-2
snooping, setting immediate leave 16-13, 35-5
ingress filtering 13-15, 32-12
internal temperature status 4-4, 20-8
IP address
BOOTP/DHCP 4-14, 37-1, 37-4, 38-2
setting 2-6, 38-2
IP port priority
enabling 14-16, 33-12
mapping priorities 14-16, 33-12
IP precedence
enabling 14-10, 33-13
mapping priorities 14-11, 33-14
IP source guard 7-5
configuring static entries 7-6, 23-14
setting filter criteria 7-7, 23-11
IPv6 traffic classes, mapping priorities 14-15, 33-17

J

jumbo frame 4-16, 20-15

L

LACP
configuration 9-8, 9-13, 26-1
local parameters 9-18, 26-10
partner parameters 9-21, 26-10
protocol message statistics 9-18, 9-21, 26-10
protocol parameters 9-13, 26-1
line profiles, VDSL 10-16, 29-35
Link Aggregation Control Protocol *See* LACP
link type, STA 12-16, 12-20, 31-21
logging
syslog traps 4-31, 20-43
to syslog servers 4-31, 20-41
log-in, Web interface 3-3
logon authentication 6-1, 22-1
RADIUS client 6-3, 22-8
RADIUS server 6-3, 22-8
TACACS+ client 6-3, 22-13
TACACS+ server 6-3, 22-13
logon authentication, sequence 6-4, 22-5, 22-7

M

main menu
CLI 18-12
web interface 3-5
Management Information Bases (MIBs) A-4
memory status 4-4, 20-12
memory utilization alarm 4-4
mirror port, configuring 9-25, 27-1
MSTP 12-1, 12-8, 31-4
global settings 12-22, 31-1
interface settings 12-18, 12-27, 31-2
multicast filtering 16-1, 35-1
multicast groups 16-9, 35-6
displaying 16-9, 35-6
static 16-9, 35-3, 35-6
multicast services
configuring 16-11, 35-3
displaying 16-9, 35-6
multicast storm, threshold 25-11
Multicast VLAN Registration *See* MVR
multicast, filtering and throttling 35-15
multicast, static router port 16-8, 35-12

Downloaded from www.Manualslib.com manuals search engine

MVR
assigning static multicast groups 16-30, 35-26
setting interface type 16-26, 35-26, 35-28
setting multicast groups 16-21, 35-24
specifying a VLAN 16-21, 35-24
using immediate leave 16-26, 35-26, 35-28

P

packet filtering 7-15, 23-5
DHCP replies 7-16, 23-9
DHCP requests 7-16, 23-8
IP/MAC address pairs 7-18, 23-5
NetBIOS traffic 7-17, 23-7
password, line 20-29
passwords 2-5, 6-1, 22-2
administrator setting 6-1, 22-2
path cost 12-5, 12-15
method 12-10, 31-9
STA 12-5, 12-15, 31-9
port authentication 6-19, 22-34
port priority
configuring 14-1, 33-1
default ingress 14-1, 33-5
STA 12-15, 31-18
port security, configuring 7-2, 23-2
port, statistics 9-29, 25-14
ports
autonegotiation 9-5, 25-5
broadcast storm threshold 9-23, 25-11
capabilities 9-5, 25-6
duplex mode 9-5, 25-3
flow control 9-5, 25-7
forced selection on combo ports 9-6, 25-8
MDI/X selection 25-9
multicast storm threshold 25-11
speed 9-5, 25-3
unknown unicast storm threshold 25-11
ports, configuring 9-1, 25-1
ports, mirroring 9-25, 27-1
priority, default port ingress 14-1, 33-5
problems, troubleshooting B-1
protocol migration 12-20, 31-24

Q

QoS 15-1, 34-1
Quality of Service *See* QoS
queue weights 14-7, 33-7

R

RADIUS, logon authentication 6-3, 22-8
rate limit
port 9-27, 28-2
setting 9-26, 28-1
setting SNMP trap 28-3
VLAN 9-28, 28-2
remote logging 4-31, 20-43
restarting the system 4-36, 19-5
RSTP 12-1, 12-8, 31-4
global configuration 12-4, 31-4
interface settings 12-18, 31-15—31-21

S

Secure Shell *See* SSH
security, client 7-1, 23-1
serial port, configuring 4-24, 20-26
SMTP, event handling 4-34, 20-48
SNMP 5-1, 21-1
community string 5-4, 21-4
enabling traps 5-6, 21-9
trap manager 5-6, 21-6
SNMPv3 5-10, 21-10—21-18
engine ID 5-11, 21-10

Downloaded from www.Manualslib.com manuals search engine

groups 5-18, 21-15
user configuration 5-12, 5-15, 21-18
views 5-24, 21-13
software
displaying version 4-7, 20-10
downloading 4-18, 20-17
Spanning Tree Protocol *See* STA
specifications, software A-1
SSH 6-10, 22-21
STA 12-1, 31-1
edge port 12-16, 12-20, 31-18
global settings, configuring 12-8, 31-3—31-10
global settings, displaying 12-4, 31-25
interface settings 12-13, 12-25, 31-16—31-24, 31-25
link type 12-16, 12-20, 31-21
path cost 12-5, 12-15, 31-16
path cost method 12-10, 31-9
port priority 12-15, 31-18
protocol migration 12-20, 31-24
transmission limit 12-10, 31-10
standards, IEEE A-3
startup files
creating 4-22, 20-17
displaying 4-18, 20-3
setting 4-18, 20-25
static addresses, setting 11-1, 30-2
statistics, port 9-29, 25-14
STP 12-1, 12-8, 31-4
Also see STA
switch settings, saving or restoring 4-20, 20-16
system clock, setting 4-37, 20-53
system mode, normal, QinQ or VLAN-swap 13-1, 20-13
system software, downloading from server 4-18, 20-17

T

TACACS+, logon authentication 6-3, 22-13
time, setting 4-37, 20-53
TPID 13-30, 32-29
traffic class weights 14-7, 33-7
trap manager 2-12, 5-6, 21-6
troubleshooting B-1
trunk
configuration 9-8, 26-1
LACP 9-11, 26-1, 26-4
static 9-9, 26-3

U

unknown unicast storm, threshold 25-11
upgrading software 4-18, 20-17
user account 6-1, 22-2
user password 6-1, 22-2, 22-4

V

VDSL 29-1
alarm profile 10-30, 29-51
automatic retraining 10-3, 29-31
band plan 10-9, 29-4
configuring switch parameters 10-1, 29-1
disabling low-end tones 10-10, 29-21
displaying chip version 20-10
displaying CPE information 10-36
displaying performance statistics 10-25, 29-82
displaying settings, signal status, communication statistics 10-21, 29-61
fast and interleaved channels 10-8, 29-24
global settings for ports 10-1, 29-2

Downloaded from www.Manualslib.com manuals search engine

ham band notch 10-8, 29-7
ham band region/usage notch 10-9, 29-9
impulse noise protection 10-10, 29-23
interface settings 10-7, 29-2
line profiles 10-16, 29-35
maximum data rate 10-10, 29-27
maximum power 10-10, 29-22
OAM functions 10-41
option band 10-9, 29-6
PSD breakpoints 10-1, 29-12
PSD frequencies at breakpoints 10-1, 29-13
PSD mask level 10-2, 29-16
PSD power level at breakpoints 10-2, 29-15
rate adaptation 10-2, 29-33
signal-to-noise margin 10-11, 29-28
upstream power back-off 10-2, 29-18, 29-19
VLANs 13-1—13-19, 32-1—32-19
802.1Q tunnel mode 13-30, 32-10, 32-27
adding static members 13-12, 13-14, 32-14
creating 13-10, 32-8
description 13-1
displaying basic information 13-7, 32-3
displaying port members 13-8, 32-16
egress mode 13-16, 32-10
interface configuration 13-15, 32-11—32-15
private 13-18, 32-17
protocol 13-20, 32-20
tag swapping 13-33, 32-30

W

Web interface
access requirements 3-1
configuration buttons 3-4
home page 3-3
menu list 3-5
panel display 3-4

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe: Contact details can be found on
www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
World Wide Web:
http://www.smc.com
http://www.smc-europe.com

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-91-352-00-40;	Fax 34-93-477-3774
UK:	44 (0) 1932 866553;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 335 5708602;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	216-712-36616;	Fax 216-71751415
North West Africa:	34 93 477 4920;	Fax 34 93 477 3774
CIS:	7 (095) 7893573;	Fax 7 (095) 789 35 73
PRC:	86-10-6235-4958;	Fax 86-10-6235-4962
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 6 238 6556;	Fax (65) 6 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-45-224-2332;	Fax 81-45-224-2331
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91-22-8204437;	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com, www.smc-europe.com, or www.smc-asia.com.

SMC® Networks

20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

Model Numbers: SMC7800A/VCP
Pub. Number: 149100012100H E012007/ST-R01

Downloaded from www.Manualslib.com manuals search engine